Gareth Greenwood

Códigos y Claves Secretas

Criptografía en BASIC

Listados para MSX, Spectrum, Amstrad, Commodore 64, Apple II

VIFI ANAYA

Códigos y claves secretas

Criptografía en BASIC

Gareth Greenwood

ANAYA MULTIMEDIA

MICROINFORMATICA

Título de la obra original:
THE MICRO CLOAK AND DAGGER BOOK

Traducción: Pedro Garre
Diseño de colección: Antonio Lax
Diseño de cubierta: Narcís Fernández

Adaptaciones para:
MSX: Gustavo Flores
Amstrad: M. A. Cebeira
Commodore: Jesús Lizaso
Apple II: Javier D. García

Publicado en Inglaterra por SIGMA PRESS
(John Wiley & Sons, Ltd.)

© EDICIONES ANAYA MULTIMEDIA, S. A., 1986
Villafranca, 22. 28028 Madrid
Depósito legal: M. 12.694-1986
I.S.B.N.: 84-7614-079-7
Printed in Spain
Imprime: Anzos, S. A. - Fuenlabrada (Madrid)

Indice

Prefacio

La escritura secreta es conocida desde tiempos inmemoriales. En el antiguo Egipto había dos tipos de escritura: La gente normal usaba la llamada escritura *demótica*, pero posiblemente para mantener en secreto los rituales religiosos, los sacerdotes usaban una forma de escritura totalmente diferente, llamada escritura *hierática*. Muchos de los líderes militares de la Antigüedad utilizaron alguna forma de escritura secreta. Los espartanos usaban un sistema llamado *escítala*, que mezclaba las letras de un mensaje para que el enemigo no pudiera leerlo si eran capturados. Julio César usaba una simple escritura secreta que cambiaba las letras del escrito de forma que quedaba aparentemente ininteligible. A lo largo de la historia siempre ha habido gente con algún motivo para guardar un secreto de ojos ajenos. Casi siempre usaron códigos y escrituras secretas para conseguir sus objetivos.

El estudio de las escrituras secretas es una ciencia por propio derecho. Se llama *criptología*. Hay dos ramas principales en la criptología, llamadas *criptografía* y *criptoanálisis*. Las palabras se derivan del griego antiguo (*Kryptos* significa secreto o escondido) e incluyen todos los métodos de codificación y cifrado que se pueden usar para hacer secreto un texto. El criptoanálisis intenta analizar qué es lo que se ha ocultado, es decir, descifrar las claves y protecciones de forma que se pueda leer el secreto del enemigo.

La criptografía y el criptoanálisis han jugado papeles muy importantes en muchos de los grandes acontecimientos de la historia, aunque no siempre se le ha dado publicidad. Esto es particularmente cierto en materia militar y diplomática. Se han ganado y perdido batallas por el descifrамiento de un mensaje. La escritura secreta ha guardado algunos de los mayores secretos políticos que el mundo ha conocido (o incluso que no ha llegado todavía a conocer).

Las grandes potencias del mundo continúan usando la criptografía, pero ésta ya no es del uso exclusivo de Gobiernos y Ejércitos. Sí —lo habrás adivinado—, los ordenadores son el motivo. Los usuarios de los ordenadores se han dado cuenta de que necesitan proteger los datos que almacenan en los bancos de datos o que transmiten a lo largo de líneas de telecomunicación. ¿Cómo pueden protegerlos? Por medio de ponerlos en clave. El *microchip* ha dado repentinamente una nueva dimensión a la criptología, y ha hecho de ella una cosa natural.

Este libro supone una introducción a la criptología para los usuarios de ordenadores personales de bajo precio. Se muestran una serie de cifrados y se acompañan los programas en BASIC, que permiten al ordenador codificar y decodificar estos mensajes. Otros programas permiten separar en distintas partes mensajes desconocidos para poder leerlos. Este libro está escrito para todos aquellos a los que les gusten los rompecabezas, ya que decodificar un mensaje no es más que un gran rompecabezas. El ordenador realiza el trabajo repetitivo, y el lector pone la inspiración. Si te interesa esto, ¡continúa leyendo y diviértete!

GARETH GREENWOOD

1
Historias del pasado

Con una gran historia tras de sí, la criptología ha tenido algunos momentos de grandeza y algunos trágicos. La historia de la criptología es realmente fascinante, y si quieres profundizar en ella te aconsejo que leas *The Codebreakers*, de David Khan, que es considerado el mejor libro histórico que se ha escrito jamás sobre este tema.

Sin embargo, dado que ningún libro de criptología estaría completo sin al menos algunas anécdotas de la historia, el autor pensó que sería una buena idea seleccionar algunas de las más sorprendentes y ponerlas en el capítulo 1, para empezar el libro con una sonrisa. Por tanto, aquí tienes las tres favoritas del autor, tres joyas perfectamente ciertas.

Había una vez (es curioso cuántas historias comienzan así) un caballero griego llamado Histiaeus. El era un emisario de la Grecia antigua a la corte persa. Los griegos y los persas no se llevaban muy bien por esa época. Por una razón o por otra, los griegos querían iniciar una revuelta. Pero Histiaeus era un diplomático, y las reglas dicen que un diplomático puede insultar a otro, pero no puede tomar parte en una lucha, luego Histiaeus necesitaba un hombre luchador.

En Grecia Histiaeus tenía un yerno llamado Aristágoras, a quien quería mandar un mensaje para que capitaneara la insurrección. El problema era que los persas no se podían enterar, luego era necesario utilizar un mensaje secreto. El hábil Histiaeus tuvo una idea inspirada. Afeitó la cabeza de un esclavo y escribió el mensaje en la calva. Tras

un tiempo, el pelo creció de nuevo y tapó el mensaje. Entonces el esclavo fue a Grecia y buscó a Aristágoras. Al verle, le dijo: "Afeita mi cabeza y lee lo que hay escrito." Cuando el pelo desapareció, Aristágoras leyó el mensaje: "Se necesitan griegos revolucionarios." Bien, no diría exactamente eso, pero así te haces una idea. Aristágoras puso manos a la obra. ¡Como puedes ver, con unos cuantos seguidores y una pequeña provisión de cabezas rapadas puedes dominar el mundo!

Un poco más cerca de nuestros días, se produjo otra historia de intrigas. Como posiblemente sabrás, las potencias europeas no siempre hemos tenido unas relaciones muy amigables entre nosotros. (Por eso se creó el Mercado Común, para dar una mejor imagen pública.) Hacia el final del siglo XVI el Imperio español tenía intereses militares y económicos en muchos puntos del "globo". El comercio marítimo requería barcos y una marina para protegerlos. No sólo los barcos necesitaban protección, también las comunicaciones militares y comerciales. Para proteger sus secretos, los marinos españoles utilizaban un código muy complicado que, creían, no se podía descubrir. Estaban equivocados.

Por una casualidad, el rey Enrique IV de Francia consiguió algunos de estos despachos españoles. No pudo entender nada y se los dio a Françoise Viete, que más tarde llegó a ser un famoso matemático, para ver si los podía descifrar. Haciendo muestra de su talento, Viete consiguió descifrar el código y leer los mensajes. Presumiblemente, gracias a los espías españoles en la Corte francesa, Felipe II se enteró pronto de que los despachos habían sido descifrados. Si hubiera tenido un poco de sentido común, habría cambiado el código, pero en lugar de eso adoptó la postura de que el código era indescifrable y que Viete tenía que haber usado magia negra para leerlo.

La magia negra era, desde luego, una herejía mortal y Felipe II decidió llevar el asunto a Roma. Como un buen católico, el Papa no era un ardiente defensor de los pecadores, pero debió quedar muy sorprendido. El Vaticano tenía su propio equipo de descifradores, y de una forma u otra consiguieron descifrar la clave española, así que el Papa vio que su propia gente había conseguido descifrar los mensajes usando la inteligencia y no las fuerzas del demonio. Felipe insistió en que Viete debía ser juzgado por sus pecados por la corte romana. El Papa encontró, al final, la típica solución política que nunca soluciona nada. Felipe no será ni el primero ni el último en caer en el error de pensar que su clave era indescifrable. Y Viete no será tampoco ni el primero ni el último en resolver con inteligencia e ingenio mensajes cifrados. La historia nos muestra un gran contraste entre la inteligencia y la incompetencia en la criptología.

El último cuento siempre hace sonreír al autor. Se refiere a un joven americano que servía en el norte de Africa, en la Segunda Guerra Mundial.

Por razones de seguridad, no estaba permitido a los soldados indicar en sus cartas dónde se encontraban en ese momento. Censores mi-

litares examinaban toda la correspondencia de los soldados para asegurarse de que se cumplían las reglas. Los soldados, rápidamente, inventaron códigos muy simples para decir a sus familiares dónde estaban. No estaban intentando descubrir ningún secreto, que es lo que pasaría si estas cartas llegaran a manos del enemigo en el camino de vuelta.

El soldado de la historia había inventado un método muy inteligente para indicar a sus padres dónde estaba. Los americanos, a menudo, usan las iniciales en sus nombres (por ejemplo, John F. Kennedy). El soldado cambiaba la inicial de en medio del nombre de su padre en la dirección de cada una de las cartas sucesivas que mandaba a casa, de forma que al final se deletrearía T.U.N.E.Z., que es donde estaba. Desafortunadamente, olvidó poner la fecha en las cartas, y éstas llegaron a casa en desorden. Sus padres, obviamente, no se dieron cuenta, ya que le escribieron diciéndole que habían sido incapaces de encontrar ZETUN en ninguno de sus atlas. ¡Tenían derecho a enfadarse!

Te habrás dado cuenta, por esta colección de historias, de que la criptología está influenciada por todas las características humanas. La historia es al fin y al cabo lo que la gente hace. No hay espacio suficiente en este libro para contarte más sobre el pasado, pero el libro del señor Khan está lleno de detalles. Si quieres más historias, léelo (te alegrarás de haberlo hecho).

De ahora en adelante, este libro es práctico. En los capítulos siguientes veremos cómo usar un ordenador personal como una máquina criptográfica y como un instrumento para el criptoanálisis.

Los programas están desarrollados en un Spectrum, pero funcionarán con alguna pequeña modificación en la mayoría de los ordenadores personales. Las claves tratadas son básicamente simples, por las obvias limitaciones de un ordenador personal. Sin embargo, se tratan la mayoría de las ideas importantes de la criptología y se dan referencias adicionales para aquellos que estén interesados.

De alguna forma, tener un ordenador personal es como tener un equipo de química. Te permite jugar con la ciencia. Con la química puedes aprender mucho, pero si te aficionas a las claves desarrollarás tu mente. Lee el resto del libro y diviértete experimentando. Recuerda que la paciencia y la determinación son las principales cualidades de todo buen "rompe-claves".

2

Uso del ordenador como una máquina de criptificación

Términos e ideas básicas

Antes de continuar, debemos dejar bien claro el significado de todos los términos que se van a utilizar. Hasta ahora, palabras como "código", "clave" y otras palabras derivadas de éstas se han usado a menudo.

Vamos a dejar claro su significado exacto:

Todos los mensajes empiezan su vida como un "texto original". Este término indica un trozo de texto en lenguaje natural, antes de que se le aplique ningún proceso para esconder su contenido. El término general para denominar a este proceso es criptificación o puesta en clave, y su efecto es transformar el texto original en el texto codificado o en el texto cifrado, dependiendo del sistema de criptificación usado.

Hay dos tipos principales de sistemas de criptificación, códigos y cifras. Cuando se usa un código, el texto original se convierte en el texto codificado al sustituir palabras o frases del texto original por palabras o números. Si el texto codificado consiste en palabras, éstas pueden consistir en cualquier secuencia de letras —no tienen por qué existir en el diccionario—. Con un código, normalmente la unidad más pequeña que se sustituye del texto original es una palabra. Por el contrario, al cifrar se opera con las letras individuales del texto original. El texto cifrado se consigue bien sustituyendo letras del texto original por otras, bien cambiando el orden de las letras, o incluso con una combinación de ambos.

La criptificación por medio de códigos se llama codificación, y por medio de cifras se llama cifrado. El proceso inverso que nos devuelve el texto original se denomina, respectivamente, decodificación y descifrado.

La lectura del contenido de un mensaje criptografiado sin conocer el método usado al ponerlo en clave, simplemente analizando el mensaje, se conoce por criptoanálisis. En este caso, el mensaje se denomina criptograma y al hecho de conseguir el texto original se llama resolución del criptograma.

Pronto te acostumbrarás a estas palabras a medida que sigas leyendo.

En este libro vamos a tratar principalmente el cifrado. Los códigos están realmente fuera del alcance de un ordenador personal, a no ser que disponga de disco. Además, el cifrado es más fácil de entender y más divertido. Vamos a examinar varios tipos de cifrado. Para cada método, encontrarás en el texto programas en BASIC para cifrar y descifrar los criptogramas. Además de los programas para cifrar y descifrar, hay otros que analizan criptogramas, para ayudarte a resolverlos si no sabes la forma en que fueron cifrados.

Primer ejemplo: **La clave del César**

Julio César utilizaba un tipo de cifrado para sus mensajes militares. Sabemos por documentos históricos que era muy simple, posiblemente el más simple de todos los métodos de cifrado. Todo lo que hacía César para producir sus textos cifrados era reemplazar cada letra del texto original por la letra que se encuentra tres posiciones después en el alfabeto. Para la X, la Y y la Z usaba la A, la B y la C. Esta simple regla se puede resumir escribiendo dos alfabetos, como se indica en la figura 1.1.

Original:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cifrado:	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Figura 1.1

En la fila superior el alfabeto empieza con la A y continúa en orden habitual. En la fila de abajo empieza con la D, continúa hasta la Z y termina en ABC. Para cifrar una letra del texto original, búscala en la fila superior y sustitúyela por la letra correspondiente de la fila del texto cifrado.

Si la frase original fueran las famosas palabras de César:

LLEGUE VI VENCI

el texto cifrado resultante sería:

OOHJXH YL YHQFL

Está bastante claro que tu ordenador se puede programar para que codifique y decodifique mensajes. Hay un programa que hace justo este trabajo:

```
  10 REM CESAR
  20 PRINT "PROGRAMA DE CIFRADO
CESAR"
  30 PRINT AT 2,2;
  40 PRINT "MODO Y CLAVE"
  50 INPUT m$
  60 IF m$(1)="0" THEN  GO TO 99
99
  70 IF m$(1)<"c" OR m$(1)>"d" T
HEN  GO TO 100
  80 IF m$(2)<"a" OR m$(2)>"z" T
HEN  GO TO 100
  90 GO TO 120
 100 PRINT AT 2,0;"? "
 110  GO TO 40
 120 PRINT AT 2,0;"MODO: ";m$(1)
;" CLAVE: ";m$(2)
 130 LET k=CODE m$(2)-CODE "a"
 140 PRINT AT 4,0;"TEXTO: ";
 150 INPUT t$
 160 IF t$(1)="0" THEN  GO TO 99
99
 170 IF m$(1)="c"  THEN  GO TO 1
90
 175 PRINT t$
 180 LET k=-k
 190 LET l=LEN t$
 195 PRINT AT 6,0;
 200 FOR i=1 TO l
 210 LET c$=t$(i)
 220 IF c$>="a" AND c$<="z" THEN
  GO TO 250
 230 PRINT " ";
 240 GO TO 280
 250 LET w=CODE c$-CODE "a"+k
 260 GO SUB 420
 270 PRINT CHR$ (w+CODE "a");
 280 NEXT i
```

```
 290 IF m$(1)="c" THEN  GO TO 99
99
 300 PRINT AT 20,2;
 310 PRINT "PULSA 's' para segui
r                  'n' para acaba
r"
 320 LET r$=INKEY$
 330 IF r$="" THEN  GO TO 320
 340 IF r$="n"  THEN  GO TO 9999
 350 IF r$="s"  THEN  GO TO 380
 360 PRINT AT 21,0;"? ";
 370 GO TO 310
 380 LET w=1-k
 390 GO SUB 420
 400 LET k=-w
 410 GO TO 195
 420 IF w<=25  THEN  GO TO 440
 430 LET w=w-26
 435 GO TO 460
 440 IF w>=0 THEN  GO TO 460
 450 LET w=w+26
 460 RETURN
9999 REM fin
```

Así es como trabaja el programa:

Líneas

20-110

1. El programa escribe el título "PROGRAMA DE CIFRADO 'CESAR'".
2. El programa te pide el modo y la clave. Consiste en una cadena formada por dos caracteres donde cada carácter individual tiene el siguiente significado:

   Primer carácter: "d" para descifrar o "c" para cifrar.

   Segundo carácter: "a" a "z": especifican la letra clave que se va a usar.

   Las letras se deben introducir en minúsculas. Si alguno de los caracteres no está en el rango adecuado, se imprime un "?" para indicar el error. Y el dato hay que volver a introducirlo. Si se introduce un "0", el programa termina.

120-130

1. Se imprimen el modo y la clave introducidos.
2. Por medio de la letra clave se halla el valor numérico de K.

Líneas	
140-160	1. El programa pide la introducción del texto original o del texto cifrado. 2. El texto se guarda en la variable t$. 3. Si el primer carácter de t$ es "0", el programa termina.
170-190	1. Dependiendo de si se está descifrando o cifrando, el valor de K se hace negativo o positivo, respectivamente.
195-280	El texto se cifra o descifra, según indique el modo de operación, y se imprime a partir de la fila 6 y la columna 0. Cualquier carácter del texto que no esté en el rango de la "a" a la "z" se imprime como un espacio en blanco.
290-410	(Se explica más adelante.)
420-460	Subrutina de aritmética en módulo 26.

El programa es extremadamente fácil de usar. Imprime un título y te pide que introduzcas la opción que desees. Hay tres elecciones: cifrado, descifrado y criptoanálisis. Empecemos con el cifrado.

Para cifrar se responde "cx", donde "x" es una letra cualquiera. Esta letra es la letra clave. La letra clave es la letra del texto cifrado que sustituirá a la letra original "a". (Julio César siempre usaba la "d", no sabemos por qué.)

No se producen variaciones muy significantes en el texto cifrado por la letra clave que se elija. Especificado el modo de cifrado y la letra clave, tienes que introducir el texto original. Una vez lo hayas tecleado, aparecerá el correspondiente texto cifrado. Ahora puedes seleccionar otra opción.

Para descifrar con la letra clave "x", simplemente teclea "dx".

El programa continúa igual que para cifrar, pero tienes que darle el texto cifrado en lugar del original, ya que este último lo produce el programa.

El cifrado de César es tan simple que todas las rutinas necesarias para cifrar, descifrar y realizar el criptoanálisis se pueden desarrollar en un pequeño programa. Realizar el criptoanálisis de un cifrado César es muy fácil. Para cada texto cifrado concreto, sólo existen 26 textos originales posibles, pues sólo hay 26 letras claves posibles. Simplemente hay que probar todas las posibilidades o, mejor aún, dejar que la máquina lo haga por ti. Tras cada desciframiento el ordenador te pregunta si quieres que continúe (teclea S o N para indicar SI o NO), y si le respondes afirmativamente vuelve a descifrar el mensaje con la siguiente letra clave en orden alfabético. En una de estas veces, si el texto original estaba en español, el texto que leas tendrá sentido. Las líneas del programa 290 a 410 hacen esto.

Prueba con estos criptogramas:

1. JQ UWNRJW JWWTW JX STWRFQ
2. DQBQFUDXA QE PQ FAZFAE
3. AJS. ¡Cuidado!
4. DWOPW KPNW

¿Qué tal te ha ido con el apartado 3? Con este criptograma tan corto hay más de una posible solución coherente. Tienes que elegir la que pienses que es correcta. (Normalmente, en los mensajes de la realidad, tienes más información en la que basarte para hacer tu elección.)

Sumario

Este capítulo trata sobre las bases de la criptografía por ordenador. Se han explicado los términos más comúnmente usados, y por medio de un cifrado muy simple has visto qué fácil es usar el ordenador para resolver criptogramas.

Una clave es una letra (en otros cifrados es una palabra o una frase) que se usa para barajar de una forma concreta el alfabeto o el texto, siguiendo una regla. En el cifrado del César, la palabra clave especifica cuántas posiciones de diferencia hay entre el alfabeto cifrado y el original.

Para resolver un criptograma de cifrado César, hay que intentar descifrarlo con todas y cada una de las claves posibles hasta que el texto resultante tenga sentido. Un texto que tenga sentido se dice que es coherente. Probar todas las claves posibles puede llegar a ser muy pesado, e intentaremos siempre que el ordenador lo haga por nosotros.

Criptogramas de práctica

Finalmente te proponemos que resuelvas los siguientes criptogramas; resuélvelos usando el cifrado del César:

1. ru iutzxgxou g igjg bkxjgj ky om
   agr jk gazktzoiu

2. fqzuqzpa qz ogqzfm cgq qx egrduy
   uqzra qe uzqjadmnxq qz xm hupm e
   uqybdq qe bdqrqdunxq cgq egrdmz
   xae pqyme m egrdud gza yueya

3. zi bzizmvg gjn cjhwmzn nji ovi x
   mzodijn lpz znj zskgdxv gv zsdno
   zixdv yz gvn hpezmzn

4. mhwhl ehl ahfukxl jnx atg bgyenb
wh xg et anftgbwtw gnxkhg lbg xq
vxivbhg vtitvxl r xgbvtvxl ihkjn
x xlmtutg wblinxlmhl t tvximtk x
e wxlmbgh

5. ti uibmuibqki bzilqkqwvit pi aql
w lmktizili acxmzili lmaxcma lmt
zmkqmvbm lmakcjzquqmvbw lm ycm
lczivbm aqotwa pmuwa makzqbw mt
vcumzw kqvkw it zmdma

3
Cifrado por sustitución monoalfabética

¡¿Qué tipo de cifrado?!

Sí, es un título bastante horrible para un capítulo, pero es el nombre correcto para el tipo de cifrados sobre los que vamos a hablar.

Alfabetos originales y cifrados

En el capítulo anterior vimos que se podía construir una tabla con el cifrado del César para decirte qué letra del texto cifrado se asignaba a cada letra del texto original. Esta tabla tenía dos alfabetos en fila, uno sobre el otro. A menudo usamos este tipo de tabla en criptografía y lo escribimos con el alfabeto original en la parte superior y el alfabeto cifrado, en la inferior.

En cada tabla alfabética, el alfabeto original está colocado en el orden normal A B C D E ... X Y Z. Un alfabeto en este orden se llama, a menudo, alfabeto normal. En el cifrado del César, el alfabeto cifrado es también un alfabeto normal, pero no se empieza por la letra A. De hecho, este alfabeto cifrado es un alfabeto normal, lo que hace que el cifrado del César sea tan fácil de descifrar.

Evidentemente, el cifrado del César no es muy usado para secretos.

¡La única forma de estar seguro de que no sean resueltos los criptogramas del César es dárselos a alguien que no sepa leer! Por tanto, podríamos pensar formas de hacer un cifrado más seguro. Una manera sencilla de hacerlo es tener un cifrado donde el alfabeto original está en orden normal, pero el alfabeto cifrado está completamente embrollado. A un cifrado de este tipo se le llama cifrado de sustitución monoalfabética. Es un cifrado de sustitución porque construye el texto cifrado sustituyendo letras del alfabeto original por letras del alfabeto cifrado. La palabra monoalfabético se utiliza debido a que sólo empleamos un único alfabeto cifrado. Veamos unos ejemplos.

Cifrado inverso al del César

Es una variación del cifrado original del César, en el cual el alfabeto cifrado está en orden inverso al normal:

Original: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cifrado: W V U T S R Q P O N M L K J I H G F E D C B A Z Y X

El problema de este cifrado es que no es una gran mejora sobre el anterior. Tenemos tan sólo 26 posibles letras clave y, por tanto, este criptograma es fácil de resolver probando todas las posibles claves. Es muy fácil modificar el programa del capítulo 2, de forma que pueda manejar igualmente alfabetos cifrados inversos. Pruébalo tú mismo.

Sustitución de alfabeto mezclado

Si estamos buscando cifrados seguros obviamente tendremos que olvidarnos de los alfabetos cifrados normales e inversos. Con 26 letras en un alfabeto hay más de 4×10^{26} formas posibles de combinarlas. Por tanto, un cifrado que utilice sólo 26 de ellas tiene que ser considerado insignificante.

Aquí es donde comienza el cifrado de claves. Puedes utilizar una palabra clave como punto de partida para producir un alfabeto mezclado. Hay dos formas de hacerlo: una, es la denominada mezcla de palabra clave y, la otra, la llamaremos mezcla y transposición de palabra clave. He aquí cómo trabajan ambas.

Mezcla de palabra clave

Para construir un alfabeto cifrado por mezcla, piensa en una palabra. A continuación escribe la palabra, pero omitiendo las letras que estén

repetidas. Entonces, escribe las letras restantes del alfabeto en el orden en el cual aparecen en el alfabeto normal. Esto te dará tu alfabeto cifrado por mezcla. He aquí un ejemplo basado en la palabra clave "CIFRAMIENTO":

C I F R A M E N T O: Palabra clave escrita sin letras repetidas.
C I F R A M E N T O B D G H J K L P Q S U V W X Y Z: Alfabeto completo.

Transposición de palabra clave

Es similar al anterior, pero en vez de escribir todas las letras en una línea, se escriben en una cuadrícula fila a fila. El alfabeto se forma leyendo las letras de la cuadrícula por columnas. Cojamos de nuevo la clave CIFRAMIENTO:

C I F R A M E N T O: Clave escrita sin letras repetidas.

C	I	F	R	A	M	E	N	T	O
B	D	G	H	J	K	L	P	Q	S
U	V	W	X	Y	Z				

Resto del alfabeto escrito en la cuadrícula.

U B C V D I W G F X H R Y J A Z K M L E P N Q T S O: Alfabeto formado leyendo hacia arriba por columnas.

De estos dos métodos el segundo es el mejor, ya que da lugar a un albafeto mejor mezclado. El método de mezcla de clave tiende a producir un alfabeto cifrado, donde las letras del final se parecen mucho a las del alfabeto original. La mezcla y transposición de clave da un poco más de seguridad.

Ahora podemos probar un cifrado por sustitución monoalfabética.

Programa de cifrado por sustitución monoalfabética

Si tienes a mano tu ordenador, puedes escribir este programa que te permite cifrar y descifrar mensajes utilizando el cifrado monoalfabético. Te permite elegir entre la mezcla de palabra clave o la mezcla de transposición de palabra clave, tanto para cifrar como para descifrar.

```
  10 REM CIFRADO MONOALFABETICO
  20 PRINT "PROGRAMA DE CIFRADO
MONOALFABETICO"
  30 PRINT AT 2,2;
  40 PRINT "MODO,MEZCLA Y CLAVE
:"
  50 INPUT m$
  60 IF m$="0" THEN  GO TO 9999
  70 LET l=LEN m$
  80 IF l<3 OR l>28 THEN  GO TO
150
  90 IF m$(1)<"c" OR m$(1)>"d" T
HEN  GO TO 150
 100 IF m$(2)<"s" OR m$(2)>"t" T
HEN  GO TO 150
 110 FOR i=3 TO l
 120 IF m$(i)<"a" OR m$(i)>"z" T
HEN  GO TO 150
 130 NEXT i
 132 PRINT AT 2,0;"MODO = ";m$(1
);
 134 PRINT " MEZCLA = ";m$(2);"
 "
 136 PRINT AT 4,0;"CLAVE : ";m$(
3 TO l)
 140 GO TO 220
 150 PRINT AT 4,0;
 160 IF l>28 THEN  GO TO 190
 170 PRINT m$
 180 GO TO 200
 190 PRINT m$( TO 28)
 200 PRINT AT 2,0;"?";
 210 GO TO 40
 220 LET m$=m$+"abcdefghijklmnop
qrstuvwxyz"
 230 LET la=LEN m$
 240 LET c$=""
 250 LET ca=CODE "a"-1
 260 DIM a$(26)
 270 FOR i=3 TO la
 280 LET as=CODE m$(i)-ca
 290 IF a$(as)<>" " THEN  GO TO
310
 300 LET c$=c$+m$(i)
```

```
 310 IF i<>1 THEN  GO TO 330
 320 LET b=LEN c$
 330 LET a$(as)="*"
 340 NEXT i
 350 IF m$(2)="s" THEN  GO TO 56
0
 360 LET d=INT (26/b)
 362 IF b*d=26 THEN  GO TO 430
 364 LET d=d+1
 365 LET lc=b*d
 400 FOR i=27 TO lc
 410 LET c$=c$+"*"
 420 NEXT i
 430 DIM a$(d,b)
 435 LET w=1
 440 FOR j=1 TO d
 450 FOR i=1 TO b
 460 LET a$(j,i)=c$(w)
 465 LET w=w+1
 470 NEXT i
 480 NEXT j
 490 LET c$=""
 500 FOR i=1 TO b
 510 FOR j=d TO 1 STEP -1
 520 IF a$(j,i)="*" THEN  GO TO
540
 530 LET c$=c$+a$(j,i)
 540 NEXT j
 550 NEXT i
 600 PRINT AT 6,0;"TEXTO :"
 610 INPUT t$
 620 PRINT AT 6,0;"          "
 630 IF t$="0" THEN  GO TO 9999
 640 LET lt=LEN t$
 650 IF m$(1)="c" THEN  GO TO 73
0
 660 DIM p$(26)
 670 FOR i=1 TO 26
 680 LET p$(CODE c$(i)-ca)=CHR$
(ca+i)
 690 NEXT i
 700 FOR i=1 TO 26
 710 LET c$(i)=p$(i)
 720 NEXT i
 725 PRINT AT 6,0;
```

```
 730 FOR i=1 TO lt
 740 IF t$(i)<"a" OR t$(i)>"z" T
HEN  GO TO 770
 750 PRINT c$(CODE t$(i)-ca);
 760 GO TO 780
 770 PRINT " ";
 780 NEXT i
9999 REM fin
```

Programa de cifrado "monoalfabético"

Líneas

20-210

1. El programa imprime el título identificador "PROGRAMA CIFRADO MONOALFABETICO".
2. El programa pide el MODO, la MEZCLA y la CLAVE. Consiste en una cadena de 28 caracteres como máximo, escritos en minúsculas, donde los caracteres individuales tienen el siguiente significado:

   Primer carácter: "d" para descifrar y "c" para cifrar.

   Segundo carácter: "s" para mezcla de clave y "t" para mezcla y transposición de clave.

   Resto: Clave de 26 letras minúsculas como máximo.

La cadena debe estar en minúsculas. Los caracteres primero y segundo deben estar en el rango que se indicó anteriormente. Si alguno de los caracteres no es adecuado, o si se introducen más de 28 caracteres, se imprime un "?" para indicar el error. Y el dato se debe volver a introducir. Cuando el MODO, la MEZCLA y la CLAVE son adecuados, las líneas 132-136 los imprimen en la pantalla. Si se introduce un "0" el programa termina.

220-340 Se forma el alfabeto cifrado en la matriz c$.

360-550 Si el método de mezcla es el de transposición de palabra clave, el alfabeto que tenemos en c$ se transpone al meterlo y volver a sacarlo de la matriz rectangular a$.

600-640 El programa pide la introducción del texto que se va a cifrar o a descifrar. Si se introduce un "0" el programa termina.

650-720 Si se está descifrando, el alfabeto cifrado se reordena de forma que cada cada elemento es el equivalente original de la

letra que ocupa la posición correspondiente en el alfabeto cifrado.

730-780 Se imprime el texto. Cualquier carácter que no esté entre la "a" y la "z" se imprime como un " ".

9999 Punto de terminación del programa.

Elige una palabra clave y prueba a cifrar los siguientes textos:

1. UN TIGRE COMIA TRIGO EN UN TRIGAL.
2. ADEMAS DE CABER HAY QUE SABER ENTRAR.
3. EL SER ABRE LA VENTANA PARA VER LA CALLE.

Si tienes un criptograma de este tipo, ¿lo podrías resolver probando todas las claves posibles? Obviamente, no (la palabra clave no tiene por qué ser coherente, y puede salir un alfabeto ordenado de forma totalmente arbitraria). El tamaño del espacio de las claves es el número de formas distintas en que se puede barajar un alfabeto. Incluso con un ordenador monstruoso necesitarías mucho más del resto de tu vida para terminar el trabajo. Incluso usando una clave coherente el trabajo es excesivo. La sustitución monoalfabética se puede descifrar muy fácilmente, pero probar todas las claves posibles no es la forma de hacerlo. Vamos a usar un método totalmente diferente...

Vuelve a cifrar los textos anteriores con una palabra clave diferente, y si antes usaste un método de mezclado, ahora usa el otro. Compara los dos textos cifrados para cada mensaje. ¿Qué observas?

Hay una cosa que está clara. Cuando repites una estructura de letras del texto original, la misma clase de estructura aparece en el texto cifrado.

Si has cifrado CABER y SABER o SER y VER, los resultados podrían ser:

NMAOR y SMAOR

o

SOR y VOR

No importa la clave que uses; estas estructuras siempre serán visibles.

Esto es importante. En la sustitución monoalfabética una letra individual siempre se representa por la misma letra en el texto cifrado. Las estructuras de las letras del texto original *siempre* aparecen en el cifrado. Esto es lo que hace posible descifrar este tipo de cifrados sin probar todas las claves. Hablaremos más sobre esto en el siguiente capítulo.

Mientras tanto, prueba unos cuantos mensajes más. Lee rápidamente el sumario y empieza el capítulo 4, que es donde empieza realmente la diversión.

Sumario

El cifrado del César es un caso simple de cifrado por sustitución monoalfabética. Tiene una variación llamada el cifrado inverso del César. Ninguno de ellos es realmente bueno, porque sólo tienen 26 claves posibles y puedes resolver criptogramas en cualquiera de ellos agotando las claves.

En general, un cifrado por sustitución monoalfabética utiliza un alfabeto cifrado que está desordenado. La mezcla de los alfabetos se puede producir a través de las palabras clave. Utilizando el método de transposición de palabras clave se puede obtener un buen alfabeto mezclado. El número de palabras clave posibles es muy amplio y el cifrado monoalfabético general lleva mucho tiempo hasta dar con todas las claves.

Notamos, no obstante, que la sustitución monoalfabética deja algunas combinaciones de letras inalteradas. Esto hará posible intentar resolver esta clase de cifrado.

Criptogramas de práctica

A continuación, te proponemos ejemplos de criptogramas monoalfabéticos para resolver:

1. sh mn ducrptns pkfn tps quc scrc
   s umhans scrhp dpahk gpacrmns bc
   spoprcacr bck tumbn anm ump epkp
   bc dushk y cmtnmacs mn tcmbrhp
   scmthbn anmtpr ghstnrhps

2. ka farfamta cd ka tuidr mo dsta
   bomstruhca para chsbuthr a tdcha
   voz

3. kiyapv tifcv kiyapyw slaptw ypyt
   tycyw kiyapyw fctyw wvrtt tn ovt
   dlart ta iay kyrtby ct dtfapt ot
   fgydttyw rita ttgtcfv oyty cfwpt
   yttwt ctn ygvt

4. tm tmims jms fifmtrs sml tatrqui
   ms naqm sfatim fifmtr nuaia jjad
   rqsa r saq ut tastrquim astunati
   m

5. xbc ab ujmjcsa yj xdjtj cjfbmbfj
   c s aby fcnwnmsajy xbcodj mb tjv
   sm tj fbwjc fdsmtb sa kbwhcj odj
   jyps yjmpstb s yd astb yj aj fs
   j dm smfas jmfnws

4

Cómo descifrar una sustitución monoalfabética

¿Estás sin aliento? Si es así, es un fallo del autor, porque hemos recorrido los tres primeros capítulos a una velocidad suicida. Ahora que tenemos el primer capítulo de resolución de criptogramas, es hora de profundizar y asentar conocimientos. Si es necesario, vuelve a los dos últimos capítulos antes de continuar. Si crees que estás preparado para lo que viene ahora, respira profundamente. Resolver criptogramas es un trabajo mucho más lento que cifrar y descifrar mensajes.

Resolución de criptogramas: la historia continúa

Ya hemos usado un método de resolución de criptogramas. Cuando vimos el criptograma del César pudimos leer algún mensaje cifrado probando todas las claves posibles. Sabemos que esto no es práctico para un cifrado monoalfabético general, pero sabemos que los criptogramas monoalfabéticos siempre muestran la estructura de las palabras del texto original. Veamos cómo esto nos ayuda a resolverlo. Supongamos que ha caído en sus manos el siguiente criptograma:

GNCFBPABCBQ IBQS AFEQ EN ABENQ Y NGTBEFFG

¿Cómo vamos a traducirlo?

La respuesta está en la estructura de las palabras. Es extraño, pero cierto, que todos los lenguajes tienen sus propias relaciones características entre letras. Estas relaciones crean los llamados contadores de frecuencia. Podemos resolver criptogramas contando el número de veces que se dan varios modelos de letras y comparando éstos, lo que podríamos suponer como "promedio" para un texto.

Contadores de frecuencia para textos del lenguaje español

Si cuentas cada vez que aparece una letra en un texto, a medida que vayas avanzando verás que cada letra responde a un porcentaje concreto del texto entero. Dentro de unos límites razonables, los porcentajes para cualquier letra son los mismos, sin importar de qué tipo de texto se trate.

En español, alrededor del 16,8 por 100 de letras en cualquier texto con una longitud razonable es la letra E. Alrededor del 12 por 100 son Aes. Luego viene la O, que cuenta con el 8,7 por 100 de todas las letras. En lo que a consonantes se refiere, la L y la S aparecen, ambas, con aproximadamente un 8 por 100. De cualquier cuenta sistemática, en una parte del texto obtendrás las cifras del porcentaje para cada letra del alfabeto. Ya se han hecho contadores de este tipo y las cifras se han publicado. Hay una tabla de frecuencias en el apéndice 1.

Más útil nos puede resultar el hecho de que los pares de letras (o digramas, como nosotros los llamamos) también se comporten así. Como para las letras solas, se han hecho contadores para ver cuántas veces aparece cada posible digrama en un texto. Los contadores de digramas son muy útiles. Tenemos tres variedades. Hay contadores de digramas, contadores de contacto derecho y contadores de contacto izquierdo. Un contador de contacto derecho cuenta, para cada letra del alfabeto, cuántas veces cada letra del alfabeto aparece a su derecha. Un contador de contacto izquierdo hace lo mismo, pero para cuando las letras aparecen en la izquierda. Si miras en el apéndice 2 encontrarás contadores de digramas, contadores de contacto derecho e izquierdo para un texto.

¡Pero hay más! También hay grupos de tres letras.

Con esos trigramas, los contadores se han compilado, pero sólo es necesario tener una tabla de los más comunes en el orden en el que es más probable que aparezcan. Esta vez observa el apéndice 3.

Aún hay otra inapreciable información al final del libro, después de los apéndices. No encontrarás sólo contadores de letras, digramas y trigramas, sino también contadores de palabras e información sobre la probabilidad que ciertas letras tienen de aparecer al principio y final de las palabras, junto con listas de palabras comunes de comienzo y fin.

¿No es maravillosa la ciencia?

Resolución de un criptograma

Adelante. Prepara papel, lápiz, goma y ponte cómodo. Vas a resolver el criptograma del principio del capítulo. Lo vamos a hacer a mano; luego, puedes utilizar el ordenador para que haga el trabajo repetitivo por ti.

Vamos a hacerlo paso a paso.

Paso 1

Escribe el criptograma en una hoja grande de papel.

Paso 2

Escribe verticalmente el alfabeto en otra hoja de papel. Recorre el criptograma y pon una marca enfrente de una letra cada vez que ésta aparezca en el criptograma. Obtendrás algo similar a la tabla siguiente:

A	*	1
B		0
C	*	1
D	*	1
E	**	2
F	*	1
G		0
H		0
I	**	2
J	*	1
K		0
L		0
M	*	1
N		0
Ñ	*	1
O	**	2
P	*****	5
Q	***	3
R		0
S	**	2
T		0
U	*	1
V		0
X		0
Y		0
Z		0
	TOTAL	24 letras

Paso 3

Esta tabla es muy irregular (compárala con la tabla del apéndice 1). Esto confirma que la sustitución es monoalfabética. Debemos continuar y examinar los digramas. Para ello necesitamos otra tabla. En este caso vamos a combinar en una única tabla los contadores de contacto izquierdo y derecho.

En esta tabla hay una columna central, con las letras ordenadas alfabéticamente. A la derecha de las letras de esta columna están las letras que aparecen a su derecha en el criptograma. A la izquierda de la columna están las letras que aparecen a la izquierda en el criptograma. El número de veces que se repite cada letra a la derecha o a la izquierda de la columna indica cuántas veces esta letra aparece en el criptograma a la derecha o a la izquierda de la letra de la columna central. En esta página tienes la tabla correspondiente al criptograma que estamos estudiando.

Paso 4

Anota todas las palabras cortas del criptograma, en su forma cifrada. En este caso tenemos tres: OS, JPS, ÑUO.

Los contadores de contacto izquierdo y derecho del criptograma son:

	A	p
	B	
	C	p
p	D	f
m p	E	i q
d	F	i
	G	
	H	
e f	I	p
	J	p
	K	
	L	
	M	e
	N	
	Ñ	u
u	O	s
q i c a j	P	s d e q q
p e p	Q	p
	R	
p o	S	
	T	
ñ	U	o
	V	
	X	
	Y	
	Z	

Con estos pocos datos ya estamos capacitados para resolver el mensaje.

Primero vamos a atacar los puntos débiles. En este criptograma está explícita la separación entre las palabras, y si hay palabras cortas es precisamente por ahí por donde hay que empezar. Observa que la letra cifrada P aparece cinco veces en todo el criptograma, y es la letra más común; esto nos permite suponer que la letra cifrada P se corresponde con la A:

OS JPS APDFI CPEIPQ ÑUO MEQPQ
-- -A- -A--- -A--A- --- ---A-

Si buscas en las tablas palabras de tres letras, con la A en posición central, verás que, por ejemplo, pueden ser VAS, HAS, PAR, MAS, TAN, LAS, DAS. Observa que la mayoría de las palabras más comunes terminan en S. Vamos, pues, a suponer que la S cifrada se corresponde con la S original.

US JPS APDFI CPEIPQ ÑUO MEQPQ
-S -AS -A--- -A--A- --- ---A-

La primera palabra sólo puede ser ES u OS. Viendo las tablas se deduce que es más probable que en ÑUO la O se corresponda con la E que con la O. Además, si fuera OS, la siguiente palabra, -AS, no tendría sentido, pues no es fácil encontrar una frase que empiece así. Por tanto, todo apunta a que la O cifrada se corresponde con la E, y viendo las tablas de los apéndices se deduce que la palabra JPS debe significar MAS:

OS JPS APDFI CPEIPQ ÑUO MEQPQ
ES MAS -A--- -A--A- --E ---A-

Dada la forma en que se hace el cifrado monoalfabético, y al ser la S una de las últimas letras del alfabeto, se puede suponer ya que la S cifrada corresponde con la S original, lo mismo ocurra con las letras T, U, V, X, Y, Z. Esto será cierto sólo en el caso de que en la palabra clave no esté ninguna de estas letras. Como ves, es necesario hacer constantemente suposiciones, que pueden ser correctas o erróneas.

Por tanto, la U se corresponde con la U, y evidentemente la palabra cifrada ÑUO tiene todas las posibilidades de ser QUE.

OS JPS APDFI CPEIPQ ÑUO MEQPQ
ES MAS -A--- -A--A- QUE ---A-

Observa ahora la tabla que hicimos de contadores de contacto izquierdo y derecho. Se ve que antes de la Q está normalmente la P, que

ya sabemos que se corresponde con la A. Dado que en estos casos PQ está al final de la palabra, y comparando con las tablas de los apéndices, parece probable que la Q se corresponda con la R.

OS JPS APDFI CPEIPQ ÑUO MEQPQ
ES MAS -A--- -A--AR QUE --RAR

Aparentemente, CPEIPQ y MEQPQ deben ser verbos, y APDFI un adjetivo. En este punto ya puede ser rentable examinar exhaustivamente todas las posibilidades.

Aunque en este ejemplo no es muy útil, se puede ver ya que la palabra clave empieza con la letra P (pues está asociada con la A) y que la O también está en la clave (pues es la única forma de que corresponda con la E). Por tanto, la longitud de la palabra clave será, como mínimo, de cinco, pues va de la A hasta la E.

Mirando las probabilidades de los digramas, vemos que las letras P, B, T, entre otras, pueden estar fácilmente a la izquierda de una R. Se ve claramente que en nuestro caso es una B, pues si no la palabra MEQPQ no tendría sentido. Por tanto, nos queda:

OS JPS APDFI CPEIPQ ÑUO MEQPQ
ES MAS -A--- -AB-AR QUE OBRAR

La palabra clave empieza por PE y su quinta letra es O. Esto sugiere, estre otras claves, la de PEDRO, que es la utilizada en nuestro caso:

Original: P E D R O A B C F G H I J K L M N Ñ Q S T U V X Y Z
Cifrado: A B C D E F G H I J K L M N Ñ O P Q R S T U V X Y Z

y el criptograma:

OS JPS APDFI CPEIPQ ÑUO MEQPQ
ES MAS FACIL HABLAR QUE OBRAR

con lo que no sólo hemos resuelto el criptograma, sino que hemos descubierto el proceso de mezcla y la clave utilizados.

Así es como se rompen los cifrados por sustitución simple.

Desde luego, llevar a cabo este proceso con papel y lápiz es bastante lento y aburrido. Como siempre, el ordenador nos es de ayuda. Para ayudarte a resolver los cifrados por sustitución monoalfabética, el capítulo termina con dos programas. El primero realiza el trabajo repetitivo por ti. Cuenta las letras y los digramas y te da las frecuencias. Veámoslo a continuación:

```
 10 REM ANALISIS DE FRECUENCIAS
 20 PRINT "PROGRAMA DE ANALISIS
DE FRECUENCIAS"
 30 PRINT AT 2,2;"TEXTO"
 40 INPUT t$
 50 IF t$="0" THEN  GO TO 9999
 60 FOR i=1 TO LEN t$
 70 IF i>LEN t$ THEN  GO TO 140
 80 IF t$(i)>="a" AND t$(i)<="z
" THEN  GO TO 140
 90 LET r$=""
100 IF i>1 THEN  LET r$=t$( TO
i-1)
110 IF i<LEN t$ THEN  LET r$=r$
+t$(i+1 TO )
120 LET t$=r$
130 GO TO 70
140 NEXT i
150 LET lt=LEN t$
160 IF lt>3 THEN  GO TO 190
170 PRINT AT 2,0;"?"
180 GO TO 40
190 PRINT AT 2,0;"TEXTO : ";t$
200 GO SUB 8000
210 LET ca=CODE "a"-1
220 DIM e(26)
230 PRINT "FRECUENCIA RELATIVA
DE LAS LETRAS:"''
240 FOR i=1 TO lt
250 LET e(CODE t$(i)-ca)=e(CODE
t$(i)-ca)+1
260 NEXT i
270 FOR i=1 TO 26
280 PRINT  INVERSE 1;CHR$ (i+ca
); INVERSE 0;": ";e(i)/lt;CHR$ 6
;
290 NEXT i
300 GO SUB 8000
310 DIM d(26)
320 FOR i=1 TO lt-1
330 IF t$(i)=t$(i+1) THEN  LET
d(CODE t$(i)-ca)=d(CODE t$(i)-ca
)+1
340 NEXT i
```

```
 350 PRINT "LETRAS REPETIDAS:"''
 360 FOR i=1 TO 26
 370 PRINT  INVERSE 1;CHR$ (i+ca
);  INVERSE 0;": ";d(i);CHR$ 6;
 380 NEXT i
 390 GO SUB 8000
 400 PRINT "FRECUENCIAS DE DOS L
ETRAS CONSECUTIVAS:"'
 410 DIM t(26,26)
 420 FOR i=1 TO lt-1
 430 LET t(CODE t$(i)-ca,CODE t$
(i+1)-ca)=t(CODE t$(i)-ca,CODE t
$(i+1)-ca)+1
 440 NEXT i
 450 FOR i=1 TO 26
 460 FOR j=1 TO 26
 470 IF t(i,j)>0 THEN  PRINT  IN
VERSE 1;CHR$ (i+ca);CHR$ (j+ca);
 INVERSE 0;": ";t(i,j);CHR$ 6
 480 IF PEEK 23689=5 AND PEEK 23
688<16 THEN  GO SUB 8000
 490 NEXT j
 500 NEXT i
 510 GO SUB 8000
 515 DIM f(26,26)
 520 PRINT "LETRAS EN ORDEN INVE
RSO:"''
 530 FOR i=1 TO 26
 540 FOR j=1 TO 26
 550 IF t(i,j)>0 AND t(j,i)=0 AN
D i<>j AND f(i,j)=0 AND f(j,i)=0
 THEN  PRINT  INVERSE 1;CHR$ (i+
ca);CHR$ (j+ca); INVERSE 0;": ";
t(i,j);CHR$ 6; INVERSE 1;CHR$ (j
+ca);CHR$ (i+ca); INVERSE 0;": "
;t(j,i): LET f(i,j)=1
 560 IF PEEK 23689=5 AND PEEK 23
688<16 THEN  GO SUB 8000
 570 NEXT j
 580 NEXT i
 590 GO SUB 8000
 600 DIM r(26,26)
 610 FOR i=1 TO 26
 620 IF e(i)=0 THEN  GO TO 660
```

```
 630 FOR j=1 TO 26
 640 LET r(i,j)=t(i,j)/e(i)
 650 NEXT j
 660 NEXT i
 670 PRINT "PROBABILIDAD CONTACT
OS           LADO DERECHO:"
 680 FOR i=1 TO 26
 690 FOR j=1 TO 26
 700 IF r(i,j)>0 THEN  PRINT  IN
VERSE 1;CHR$ (i+ca);CHR$ (j+ca);
 INVERSE 0;": ";r(i,j);CHR$ 6
 710 IF PEEK 23689=5 AND PEEK 23
688<16 THEN  GO SUB 8000
 720 NEXT j
 730 NEXT i
 740 GO SUB 8000
 750 DIM l(26,26)
 760 FOR i=1 TO 26
 770 IF e(i)=0 THEN  GO TO 810
 780 FOR j=1 TO 26
 790 LET l(i,j)=t(j,i)/e(i)
 800 NEXT j
 810 NEXT i
 820 PRINT "PROBABILIDAD CONTACT
S LADO IZQUIERDO:"
 830 FOR i=1 TO 26
 840 FOR j=1 TO 26
 850 IF l(i,j)>0 THEN  PRINT  IN
VERSE 1;CHR$ (j+ca);CHR$ (i+ca);
 INVERSE 0;": ";l(i,j);CHR$ 6
 860 IF PEEK 23689=5 AND PEEK 23
688<16 THEN  GO SUB 8000
 870 NEXT j
 880 NEXT i
 890 GO SUB 8000
 900 DIM g(26,lt)
 910 FOR i=1 TO 26
 920 FOR j=2 TO lt-1
 930 IF t$(j)=CHR$ (i+ca) THEN
LET g(i,j)=1
 940 NEXT j
 950 NEXT i
 960 PRINT "GRUPOS DE TRES LETRA
S CONSECUTIVAS:"
```

```
 970 FOR i=1 TO 26
 980 IF e(i)=0 OR (e(i)=1 AND (t
$(1)=CHR$ (i+ca) OR t$(1t)=CHR$
(i+ca))) THEN  GO TO 1050
 990 PRINT  INVERSE 1;CHR$ (i+ca
); INVERSE 0;": ";
1000 FOR j=2 TO 1t
1010 IF g(i,j)=1 THEN  PRINT t$(
j-1 TO j+1);",";
1020 NEXT j
1030 PRINT CHR$ 8;" "
1040 IF PEEK 23689<6 THEN  GO SU
B 8000
1050 NEXT i
1060 GO SUB 8000
1070 GO TO 9999
8000 PRINT AT 21,0;"PULSE CUALQU
IER TECLA (C=COPY)."
8010 LET r$=INKEY$
8020 IF r$="" THEN  GO TO 8010
8030 IF r$<>"c" THEN  GO TO 8060
8040 COPY
8050 GO TO 8010
8060 IF r$="0" THEN  GO TO 9999
8070 CLS
8080 RETURN
9999 REM fin
```

Anotaciones para el "programa de análisis de frecuencias"

Líneas	
10-20	Comentario identificador del programa e impresión del título.
30-50	Pide la introducción del texto que se va a analizar; lee el texto; salta al fin del programa si texto = "0".
60-140	Se eliminan los espacios del texto.
150-180	En el texto debe haber, al menos, cuatro caracteres distintos de espacio: si no es así, el usuario debe introducir un texto más largo.
190	Se imprime el texto.

Líneas	
200	Se pregunta al usuario si desea continuar, imprimir, etc. (Mira los comentarios de las líneas 8000 a 8080.)
210-290	Se calculan las frecuencias de las letras individuales y se imprimen; las frecuencias se dan según la proporción respecto al número total de caracteres del texto.
300	Se pregunta al usuario si desea continuar, imprimir, etc.
310-380	Se calculan e imprimen las frecuencias de letras dobles; las frecuencias representan simplemente el número de apariciones.
400-500	Se calculan e imprimen las frecuencias de digramas.
515-580	Se calculan e imprimen las frecuencias inversas.
600-730	Se calculan e imprimen las frecuencias relativas de contacto derecho; las frecuencias son proporcionales a las letras de contacto derecho.
750-880	Se calculan e imprimen las frecuencias relativas de contacto izquierdo; las frecuencias son proporcionales a las letras de contacto izquierdo.
900-1050	Se calculan e imprimen las frecuencias de los trigramas.
1070	Salta al final del programa.
8000-8080	Rutina de lectura; un ciclo espera la pulsación de un tecla; si se lee una "c" se copia la pantalla; termina si es un "0" (en cualquier otro caso el programa continúa).
9999	Línea de fin de programa.

Instrucciones de uso del "programa de análisis de frecuencias"

El programa "Análisis de frecuencias" calcula unas estadísticas básicas para el trozo de texto introducido. Las estadísticas son:

1. La frecuencia relativa de cada letra.
2. Las frecuencias de pares de letras.
3. Las frecuencias de las digramas.
4. Las frecuencias inversas.
5. Las probabilidades de contacto derecho (es decir, las frecuencias relativas de contacto derecho).
6. Las probabilidades de contacto izquierdo (es decir, las frecuencias relativas de contacto izquierdo).
7. Un contador de trigramas.

El programa pide la introducción del texto, y el usuario teclea el texto que desea analizar. En primer lugar, se calculan e imprimen las frecuencias de letras individuales. Después se continúa con letras dobles, digramas, inversos, contacto derecho e izquierdo y trigramas, en este orden. Cuando se termina cada tipo de análisis se pide al usuario que indique si desea continuar. Esto se hace pulsando cualquier tecla, excepto la "c". Si se teclea "c" se vierte el contenido de la pantalla a la impresora.

Algunas frecuencias representan el número absoluto de apariciones (dobles, digramas, inversos y trigramas). El resto son frecuencias relativas (es decir, proporciones del total). Esto hace que la información de salida sea más fácil de usar en conjunción con las tablas de los apéndices.

El usuario puede terminar con el programa en cualquier momento, pulsando "0" cuando se pida la introducción de una tecla.

El programa "Ayuda monoalfabética" es bastante más sofisticado. Utiliza métodos estadísticos para sugerir las letras más probables en ciertos puntos del criptograma.

El programa dispone de una gran tabla de probabilidades de contacto derecho, derivada de las tablas de los apéndices. Utiliza ésta para hallar las probabilidades de posibles combinaciones de letras, e imprime las probabilidades por pantalla. De esta forma se evita que el usuario tenga que hacer estos cálculos por sí mismo.

El método de cálculo está basado en algunos conceptos estadísticos que se encuentran fuera del alcance de este libro. Si quieres estudiar la justificación matemática de estos cálculos, examina el libro de Alan Konheim.

El método utilizado no es de los más potentes, especialmente respecto a los que calculan "la probabilidad relativa de un texto original". Sin embargo, el problema era conseguir un tiempo de ejecución aceptable. Si tienes acceso a un ordenador de, por ejemplo, 16 bits, y puedes programarlo en un lenguaje compilado, puedes intentar adaptar el programa para que calcule las estadísticas sugeridas por Konheim.

En criptogramas extensos, los métodos basados en probabilidades relativas del texto original pueden prácticamente producir la solución de forma automática (pero hay que programarlos cuidadosamente para producir una velocidad y una eficiencia aceptables).

Veamos ahora el programa "Ayuda monoalfabética":

```
  10 REM AYUDA MONOALFABETICA
  20 PRINT AT 11,4;"PONGA LA CIN
TA CON DATOS";AT 12,3;"PULSE LUE
GO CUALQUIER TECLA"
  30 BEEP 1,12
```

```
  40 IF INKEY$="" THEN  GO TO 40
  50 LOAD "" DATA e()
  60 LOAD "" DATA t()
  70 CLS
  80 PRINT "PROGRAMA DE AYUDA MO
NOALFABETICA"
  90 PRINT AT 2,2;"TEXTO"
 100 INPUT t$
 110 IF t$="0" THEN  GO TO 9999
 120 LET lt=LEN t$
 130 IF lt>9 THEN  GO TO 160
 140 PRINT AT 2,0;"?"
 150 GO TO 100
 160 FOR i=1 TO lt
 170 IF t$(i)<"a" OR t$(i)>"z" T
HEN  LET t$(i)=" "
 180 NEXT i
 190 PRINT AT 2,0;"TEXTO : ";t$
 200 LET b1=6+INT ((lt-1)/15)
 210 DIM c(26)
 220 LET ca=CODE "a"-1
 230 FOR i=1 TO lt
 240 IF t$(i)<>" " THEN  LET c(C
ODE t$(i)-ca)=c(CODE t$(i)-ca)+1
/lt
 250 NEXT i
 260 GO SUB 8000
 265 CLS
 270 FOR i=1 TO 26
 280 PRINT  INVERSE 1;CHR$ (i+ca
); INVERSE 0;": ";c(i),
 290 NEXT i
 300 GO SUB 8000
 310 LET a$="********************
*******"
 315 LET b$=a$
 320 CLS
 330 PLOT 20,172
 340 DRAW 216,0
 350 DRAW 0,-24
 360 DRAW -216,0
 370 DRAW 0,24
 380 PRINT AT 1,3;"abcdefghijklm
nopqrstuvwxyz";AT 2,3;a$'
```

```
 385 LET p$=""
 390 FOR i=0 TO 15*INT ((lt-1)/1
5) STEP 15
 400 LET j=15
 410 IF i+j>lt THEN  LET j=lt-i
 420 PRINT 't$(i+1 TO i+j);TAB 1
6;
 430 FOR j=1 TO j
 440 LET c$=" "
 450 IF t$(i+j)<>" " THEN  LET c
$=a$(CODE t$(i+j)-ca)
 460 LET p$=p$+c$
 470 PRINT c$;
 480 NEXT j
 490 NEXT i
 500 PRINT AT 21,0;"PULSE b,c,d,
e,f,n,p,s,t OR 0"
 510 LET r$=INKEY$
 520 IF r$="" THEN  GO TO 510
 530 PRINT AT 21,0;TAB 31
 540 IF r$<>"b" THEN  GO TO 920
 550 GO SUB 8100
 560 GO SUB 8200
 570 PRINT  INVERSE 1;CHR$ (1+64
); INVERSE 0;": ";"Frecuencia: "
;c(1),
 575 IF c(1)=0 THEN  GO TO 910
 580 LET b=1
 590 FOR i=1 TO 26
 600 IF ABS (e(i)-c(1))>b THEN
GO TO 630
 610 LET b=ABS (e(i)-c(1))
 620 LET p=i
 630 NEXT i
 640 PRINT ,"Sugerencia: "; INVE
RSE 1 AND b$(p)="*";CHR$ (p+ca);
 INVERSE 0'"Transiciones:",
 650 DIM n(26)
 660 FOR i=2 TO lt
 670 IF t$(i)<>1$ THEN  GO TO 80
0
 680 LET j=0
 683 LET j=j+1
 687 IF i-j<1 THEN  GO TO 800
```

```
 690 IF p$(i-j)="*" THEN  GO TO
800
 695 IF p$(i-j)=" " THEN  GO TO
683
 700 LET t=CODE p$(i-j)-ca
 710 FOR j=1 TO 26
 720 LET n(j)=n(j)+t(t,j)
 730 NEXT j
 800 NEXT i
 810 FOR i=2 TO (19-b1)*2
 820 LET b=0
 830 FOR j=1 TO 26
 840 IF n(j)<=b THEN  GO TO 870
 850 LET b=n(j)
 860 LET p=j
 870 NEXT j
 880 IF b=0 THEN  GO TO 910
 890 PRINT  INVERSE 1 AND b$(p)=
"*";CHR$ (p+ca); INVERSE 0;": ";
n(p),
 895 LET n(p)=0
 900 NEXT i
 910 GO TO 500
 920 IF r$<>"c" THEN  GO TO 950
 930 COPY
 940 GO TO 500
 950 IF r$<>"d" THEN  GO TO 990
 960 GO SUB 8200
 965 IF a$(1)<>"*" THEN  LET b$(
CODE a$(1)-ca)="*"
 970 LET a$(1)="*"
 980 GO TO 320
 990 IF r$<>"e" THEN  GO TO 1040
1000 GO SUB 8100
1010 GO SUB 8200
1020 PRINT 1$;": ";e(1)
1030 GO TO 500
1040 IF r$<>"f" THEN  GO TO 1090
1050 GO SUB 8100
1060 GO SUB 8200
1070 PRINT 1$;": ";c(1)
1080 GO TO 500
1090 IF r$="n" THEN  GO TO 310
1100 IF r$<>"p" THEN  GO TO 1200
```

```
1110 GO SUB 8100
1120 INPUT "Letras?";l$
1130 IF l$="0" THEN  GO TO 9999
1140 IF LEN l$<>2 THEN  GO TO 11
20
1150 LET l1=CODE l$(1)-ca
1160 LET l2=CODE l$(2)-ca
1170 IF l1<1 OR l1>26 OR l2<1 OR
 l2>26 THEN  GO TO 1120
1180 PRINT l$;":";t(l1,l2)
1190 GO TO 500
1200 IF r$<>"s" THEN  GO TO 1240
1210 FOR i=4 TO 21
1213 PRINT AT i,0;TAB 31;" "
1217 NEXT i
1220 PRINT AT 4,0;p$
1230 GO TO 9999
1240 IF r$<>"t" THEN  GO TO 1340
1250 GO SUB 8200
1260 LET q$=l$
1270 LET l1=l
1280 GO SUB 8200
1300 IF b$(l)<>"*" THEN  GO TO 1
280
1310 IF a$(l1)<>"*" THEN  LET b$
(CODE a$(l1)-ca)="*"
1320 LET a$(l1)=l$
1325 LET b$(l)=q$
1330 GO TO 320
1340 IF r$="0" THEN  GO TO 9999
1350 PRINT AT 21,0;"?"
1360 BEEP 1,0
1370 GO TO 500
8000 PRINT AT 21,0;"PULSE CUALQU
IER TECLA (C=COPY)."
8010 LET r$=INKEY$
8020 IF r$="" THEN  GO TO 8010
8030 IF r$="0" THEN  GO TO 9999
8040 IF r$<>"c" THEN  RETURN
8050 COPY
8060 GO TO 8010
8100 FOR i=b1 TO 21
8110 PRINT AT i,0;TAB 31;" "
8120 NEXT i
```

```
8130 PRINT AT b1,0;
8140 RETURN
8200 INPUT "Letra?";1$
8210 IF 1$="0" THEN  GO TO 9999
8220 IF LEN 1$<>1 THEN  GO TO 82
00
8230 LET 1=CODE 1$-ca
8240 IF 1<1 OR 1>26 THEN  GO TO
8200
8250 RETURN
9999 REM fin
```

Anotaciones para el programa "Ayuda monoalfabética"

Líneas	
10-60	Inicialización del programa. Se cargan de la cinta las tablas de frecuencias de letras individuales y de probabilidad de contacto derecho.
70-190	Se lee el texto, y los caracteres no válidos (los que no están entre la "a" y la "z") se sustituyen por espacios. A continuación, se imprime el texto en la pantalla.
200-250	Se calculan las frecuencias de las letras y se almacenan en la matriz "c".
260	El usuario pulsa una tecla para indicar que desea continuar.
265-490	Se imprimen el alfabeto original y el alfabeto cifrado correspondiente (inicialmente todo son "*"). A continuación se imprime por grupos de letras el texto, según la equivalencia dada por los alfabetos anteriores.
500-530	Se lee una tecla.
540-910	La rutina pide la introducción de un carácter y muestra el alfabeto equivalente basado en la comparación de la frecuencia observada y la frecuencia esperada de las letras y de contacto derecho (todas frecuencias relativas).
920-940	Copia la pantalla en la impresora como respuesta a la pulsación de la tecla "c".
950-980	Borra una letra de prueba del alfabeto cifrado (es decir, cambia un par de pruebas).
990-1030	Imprime la frecuencia relativa esperada de una letra del texto original.
1040-1080	Imprime la frecuencia relativa observada en una letra del texto cifrado.

Líneas	
1090-1190	Imprime la frecuencia relativa de contacto derecho esperada para un par de letras del texto original.
1200-1230	Imprime el texto original reconstruido hasta el momento y sale.
1240-1330	Asigna una equivalencia original-cifrado de prueba, por medio de la inserción de una letra en el alfabeto cifrado.
1340-1370	Se ha producido un error y se vuelve a pedir la introducción de una tecla.
8000-8060	Rutina de lectura de una tecla. Vuelca la pantalla en la impresora si se pulsa una "c".
8100-8140	Rutina de borrado de la pantalla usada por el procedimiento principal de impresión.
8200-8250	Rutina de lectura y comprobación de una letra.
9999	Línea de terminación del programa.

El programa es fácil de usar. Hay tres modos básicos de operación.

Para empezar, el programa necesita leer dos tablas que contienen las probabilidades relativas de letras individuales y de contacto derecho. Tienes que grabar estas matrices en la cinta por ti mismo. Hay un programa que hace esto al final el libro. Asegúrate de que la cinta que uses tenga el programa "Ayuda monoalfabética" y las dos tablas (la de letras primero y la de contacto derecho después, en este orden). El programa será capaz de funcionar siempre, sin ninguna modificación en la cinta.

Se lee el texto y el programa actúa según la tecla que a continuación pulse el usuario, como se indica:

Tecla	*Acción*
b	Imprime el estado actual de las pruebas de desciframiento.
c	Copia la pantalla en la impresora.
d	Borra una equivalencia original-cifrado.
e	Imprime las frecuencias relativas esperadas de las letras.
f	Imprime las frecuencias relativas observadas en el texto cifrado.
n	Borra los alfabetos y empieza de nuevo.
p	Imprime las probabilidades relativas de contacto derecho para un par de letras.
s	Imprime el texto original final.
t	Prueba una equivalencia original-cifrado (es decir, sustituye una letra de prueba).
0	Finalización.

Criptogramas de práctica

A continuación tienes algunos criptogramas con los que puedes usar estos programas. Deberás encontrar el modo más productivo:

1.
```
jos  nqfkgqqos  dmldjusfmlgs  ag  jo
flvgstfcodfml  mqaagloaonmmq  g j kf
lfstgqfm  aggj  fltgqfmq  smrqg nqqgs
ullos  fknjfdodfmlgss  gl  gj  tqobfd
m  ag  aqmco  ag  kfgkrqms  ag  jms  dul
qqnms  ag  sgcuqfaoa  gl  dgulo  onul
to  o  kfgkrqms  ag  jo  nmjrdfo  lodf
mloj
```

2.
```
de  nwopfdaw  de  darygnvw  nxelxfye
dxfwrdw  ndedulfyhw  hxfyoldewa  xe
lvcwa  lfda  hvya  do  cyhfvh  ldfcvo
w  ybdf  nwo  ey  ednlxfy  hde  cyovtv
dalw  hd  cyhfvh
```

3.
```
hf  djropjftdkjfh  qktdfhdqrf  cf  i
fjdloqrfbk  qs  pkrsjbk  potcfzk  f
rkbk  mpkapfif  bo  boqfppkhhk  fpif
iojrdqrf  oj  oh  oqmftdk  y  oj  oqmo
tdfh  fh  mpkyotrk  jkprofiopdtfjk
bo  djdtdfrdvf  bo  bolojqf  oqrpfro
adtf
```

4.
```
ewqbwqvswi  pw  owsihqvi  avq  switr
bvph  ytwsbvi  ptsvqbw  rhi  trbxyhi
 pxvi  v  evtiv  pw  rhi  jxhrwqbhi  b
xmhqwi  ztw  avq  vmwebvph  rv  ehibv
 hsxwqbvr  pw  rv  xqpxv  k  rvi  swfx
hqwi  ewqbsvrwi  pw  jxwbqvy  k  mxrx
oxqvi  yxrrhqwi  pw  owsihqvi  owspx
wshq  iti  ahfvswi  h  btjxwshq  ztw
atxs  v  dhqvi  yvi  iwftsvi
```

5.
```
jnr  gnmtugsnqar  pua  cdydm  embaqe
tn  djgncnj  y  radm  qapuaqetnr  onq
 jd  onjeged  odqd  pua  ra  rnkasdm
d  jd  oquaid  ta  jd  djgncnjakedd  ra
buqdkamsa  cdqdm  ieam  am  mabdqra
d  rnojdq  am  aj  bjniesn  gnqqaronm
teamsa  reakoqa  pua  am  arsa  gdrn
dgaosam  jd  rdmgenm  pua  oqngatd  j
d  nsqd  rnjugenm  ar  mn  iaiaq  dmsa
r  ta  gnmtugeq
```

5
Cifrados por transposición

En este capítulo veremos un tipo diferente de cifrado. Hemos visto los cifrados por sustitución donde el texto cifrado se obtiene reemplazando cada letra del texto original por su equivalente en el texto cifrado. Ahora veremos otro tipo de cifrado, donde obtendremos el texto cifrado mezclando el orden de las letras en el texto original. Este tipo de cifrado se llama "cifrado por transposición".

La forma más simple de cifrado por transposición se llama cifrado zig-zag o *railfence*. Este es, de alguna forma, un complemento del cifrado del César, ya que usa una clave, de las pocas posibles, como base para barajar las letras.

Cifrado zig-zag: un ejemplo

Para cifrar un mensaje usando este cifrado, debe escribir primero en forma de zig-zag, como en el siguiente diagrama. La clave es la profundidad de zig-zag que usa. Para ver lo que significa, el diagrama muestra cómo se escriben las famosas palabras del César en un zig-zag de profundidad tres:

```
L       U       V       I
  L   G   E   I   E   C
    E       V       N
```

Para generar el criptograma escriba debajo las letras en el orden en el cual se dan cuando lee el diagrama zig-zag línea a línea, de izquierda a derecha. En este ejemplo el texto cifrado correspondiente es:

LUVIL GEIEC EVN

Naturalmente, la transposición destruye las separaciones entre las palabras, por lo que a menudo escribimos los textos cifrados por transposición en grupos regulares, normalmente de cinco letras cada uno.

Probablemente es el mejor conocido y también el cifrado menos seguro por transposición. El punto débil viene a ser el pequeño tamaño del espacio de las claves, el cual está normalmente en el rango de 2 a k, donde k es la mitad de la longitud del mensaje.

A no ser que el mensaje sea largo, esto da un relativo pequeño espacio de claves, y los criptogramas zig-zag se resuelven fácilmente probando todas las claves posibles.

Un programa para el cifrado zig-zag

Dando por hecho que usted es una persona culta, habrá supuesto que es fácil proponer un programa para cifrar, descifrar y romper los criptogramas de zig-zag. A continuación hay un listado que permite trabajar en líneas similares al programa del cifrado del César del capítulo 2. Déle un vistazo y opine.

```
  10 REM ZIG ZAG
  20 PRINT "PROGRAMA DE CIFRADO
'ZIG ZAG'"
  30 PRINT AT 2,2;"MODO Y CLAVE"
  40 INPUT m$
  50 IF m$="0" THEN  GO TO 9999
  60 IF LEN m$<2 THEN  GO TO 110
  70 IF m$(1)<"c" OR m$(1)>"d" T
HEN  GO TO 110
  75 FOR i=2 TO LEN m$
  80 IF m$(i)<"0" OR m$(i)>"9" T
HEN  GO TO 110
  90 NEXT i
 100 GO TO 130
 110 PRINT AT 2,0;"?"
 120 GO TO 40
 130 LET k=VAL m$(2 TO )
 140 IF k<2 THEN  GO TO 110
```

```
 150 PRINT AT 2,0;"MODO : ";m$(1
);" CLAVE : ";k
 160 PRINT AT 4,2;"TEXTO"
 170 INPUT t$
 171 FOR i=2 TO LEN t$
 172 IF i<LEN t$ THEN  IF t$(i)=
" " THEN  LET t$=t$( TO i-1)+t$(
i+1 TO ): GO TO 172
 173 NEXT i
 175 IF t$="0" THEN  GO TO 9999
 180 LET lt=LEN t$
 190 IF lt>0 THEN  GO TO 220
 200 PRINT AT 4,0;"?"
 210 GO TO 170
 220 PRINT AT 4,0;"TEXTO : ";t$
 230 PRINT
 240 LET s=2*(k-1)
 250 IF m$(1)="d" THEN  GO TO 39
0
 260 FOR i=1 TO lt STEP s
 270 PRINT t$(i);
 275 NEXT i
 280 FOR i=1 TO k-2
 290 FOR j=1 TO lt STEP s
 300 IF j+1<=lt THEN  PRINT t$(j
+i);
 310 IF j+s-i<=lt THEN  PRINT t$
(j+s-i);
 330 NEXT j
 340 NEXT i
 350 FOR i=k TO lt STEP s
 360 PRINT t$(i);
 370 NEXT i
 380 GO TO 9999
 390 DIM c$(lt)
 400 LET l=0
 410 FOR i=1 TO lt STEP s
 420 LET l=l+1
 430 LET c$(i)=t$(l)
 440 NEXT i
 450 FOR i=1 TO k-2
 460 FOR j=1 TO lt STEP s
 470 IF j+i>lt THEN  GO TO 500
 480 LET l=l+1
```

```
 490 LET c$(i+j)=t$(l)
 500 IF j+s-i>lt  THEN  GO TO 54
0
 510 LET l=l+1
 520 LET c$(j+s-i)=t$(l)
 540 NEXT j
 550 NEXT i
 560 FOR i=k TO lt STEP s
 570 LET l=l+1
 580 LET c$(i)=t$(l)
 590 NEXT i
 600 PRINT c$
 610 PRINT AT 20,2;"Pulse 's' pa
ra seguir                 'n' pa
ra detenerse"
 620 LET r$=INKEY$
 630 IF r$="" THEN  GO TO 620
 640 IF r$="s" THEN  GO TO 680
 650 IF r$="n" THEN  GO TO 9999
 660 PRINT AT 21,0;"?"
 670 GO TO 620
 680 LET k=k+1
 690 PRINT AT 2,17;k
 700 GO TO 220
9999 REM fin
```

Programa de cifrado "zig-zag". Anotaciones e instrucciones de uso

Líneas	
10-20	Comentario identificador del programa e impresión del título.
30-140	Pregunta el modo y la clave. Si se introduce un "0" termina; los modos son "c" y "d"; vuelve a pedir la introducción de datos si se produce algún error.
150-170	Imprime el modo y la clave, y pide la introducción del texto.
171-210	Quita los espacios del texto. Si se introduce un "0" termina. Comprueba que el texto tenga al menos un carácter distinto de espacio. Si hay algún error vuelve a leer el texto.

Líneas	
220-240	Imprime el texto e inicializa los procedimientos de cifrado.
250	Selecciona entre el proceso de cifrado o el de descifrado.
260-370	Imprime el texto cifrado en forma de diagonales (por medio de tres bucles FOR).
380	Salta al fin del programa.
390-610	Rutina de análisis-desciframiento. Imprime el texto descifrado por diagonales.
620-700	Rutina de lectura de las instrucciones del usuario. Se está en un ciclo hasta que se pulsa una tecla; "n" produce la terminación, "s" hace que se incremente en uno la profundidad y vuelve a intentar realizar el descifrado con una nueva clave. Si la tecla no es la adecuada el ciclo continúa.
9999	Fin del programa.

Instrucciones de uso para el programa de cifrado "zig-zag"

Para empezar, el programa pide el modo y la clave. El modo puede ser "c" o "d", para cifrar y descifrar, respectivamente. La clave es la profundidad del método. Debe ser un número entero positivo. El modo y la clave se deben introducir como una cadena única (por ejemplo, "e8"). Si se produce algún error, el programa vuelve a pedir la introducción de los datos, imprimiendo un signo de interrogación.

Tras aceptar el modo y la clave, el programa pide el texto. Debe contener, al menos, un carácter distinto de espacio (el programa quita todos los espacios). De nuevo, si se detecta un error, se pide la reintroducción del texto.

Si el modo seleccionado es el de cifrado, el programa imprime el texto original y el cifrado. Si el modo es el de descifrado, se imprime el texto cifrado seguido de un descifrado inicial hallado por medio de la clave introducida por el usuario. Se pide al usuario que indique si quiere continuar. Si es así, se incrementa en uno el número de la clave y se vuelve a hacer otro intento de desciframiento.

Como en todos los programas de este libro, el usuario puede salir del programa tecleando "0" cuando se le pide.

Criptogramas de práctica

A continuación te damos una serie de criptogramas para que practiques con el programa Zig-zag:

1. e t v e o c a r h r s i a d s c n a o t l d d e o e f r o d e t
   m g q e u g n n p r i a e j d e i u l d s u i r n u t o o a m r
   n o e o l h s i i a d d s n e m s e s o a o u j e a u a a t d d
   a e r z g a a a

2. l a i e a s r s o e s n i u a s s c c i e n p c t e p e m c l e
   m i n i t e e a e r a a f m l a d l m r a o g u o d h m r s a b
   e s r o c y m y r a i f c i n o s s e n o t m l r u n o i m o u
   d p r a e e a g i n u e g d e u r o n e d e p z r h c r a g r s
   s i s a i n p e b m i e s a o t a o n t c e a a t p e e n r u s
   r o n a s m a a g a

3. q e r r e u t c a o s a u r c t h u l s e v t e c p e n c o e u
   u n n s e q t d l c t a u h e r l o e e e t a n l n c d p e g j
   c c t a t r u l e o i e t m o s a e n c u l n l e a o i n r y s
   e i n o v e o e a r s o s a e m s t d o r i o c o o u o s m r e
   n d a a r

4. e a s r u e r n d z s i o o e e d o s l t e e a e q e n s o t u
   d a u a o o e m a b n t m d h d p o u l s t n i i d s n a l e v
   f u n e n r r n p o a c i d n o n a n e l r n h o e e d i n m s
   l i e r n e s u e o q o m n a m a o r e m e n r o o o y o r a g
   e i o o u o e a n c y z c u n e a u e d r i i b i a e s s m s s
   l r n n p t d s q h c t e a o a e e o o i s d a p r b r b d v q
   e b e o a a o a a i r d y d a y e e e u r

5. l a t a a l l a o p d h u r t a a o c s n l d m o u e a e b a p
   i b u r r e m r f e a n a a p s

6

Cifrado por transposición de bloques

Si te asustas es que te has saltado el capítulo 5, pero no importa. Realmente la utilidad de un cifrado como el zig-zag es muy limitado.

Hay muchos cifrados por transposición que dan buenos resultados, y en este capítulo se examinan algunos de ellos. Todas las claves de este capítulo son de las que escribes el texto original en una red rectangular y, a continuación, sacas las letras en un orden diferente al que lo escribiste.

Este método de cifrado es muy fácil y rápido, incluso con papel y lápiz, y por esto los sistemas de transposición son adoptados frecuentemente por los ejércitos para su uso en el campo de batalla. El libro de David Khan, *The Codebreakers*, contiene varios casos de utilización de estas claves en la Primera Guerra Mundial.

Cuando se usa la transposición, ésta puede ser completa o incompleta. Si es completa, la red rectangular en la que se escribe el texto se rellena hasta el final, para hacer que la longitud del texto coincida con el número de cuadros de la red. El método de transposición completa de columnas es el más fácil y, por tanto, empezaremos por él.

Transposición completa de columnas

Supongamos que queremos cifrar el texto:

NUNCA EN LA HISTORIA HA HABIDO TAN POCOS DOMINANDO TANTO A TANTOS

El texto contiene 54 letras, luego elegimos una red de 12 filas y 5 columnas, en la que las 54 letras caben sin dejar demasiados cuadrados sin utilizar, tan sólo seis. El texto se puede escribir como se indica en la figura 6.1.

Paso 1 Se escribe el texto en la red y la palabra clave, arriba:

H	U	M	O	S
N	U	N	C	A
E	N	L	A	H
I	S	T	O	R
I	A	H	A	H
A	B	I	D	O
T	A	N	P	O
C	O	S	D	O
M	I	N	A	N
D	O	T	A	N
T	O	A	T	A
N	T	O	S	I
H	N	T	O	S

Figura 6.1

Los seis espacios que quedan en la red los llenamos con las letras I, H, N, T, O, S, ya que aparecen en el mensaje y harán éste más difícil de descifrar.

Cuando el texto esté escrito en la red, las columnas se mezclan siguiendo alguna regla. Una vez más vamos a usar una palabra clave que debe tener el mismo número de letras que columnas tiene la red. En este ejemplo vamos a usar la palabra HUMOS. La palabra clave se escribe en la parte de arriba de la red. A continuación, se cambian las columnas de orden, incluyendo las letras de la palabra clave, de forma que las letras de la palabra clave aparezcan en orden alfabético, como muestra la figura 6.2.

Paso 2 Las columnas se reordenan para poner las letras de la palabra clave en orden alfabético:

H	M	O	S	U
N	N	C	A	U
E	L	A	H	N
I	T	O	R	S
I	H	A	H	A
A	I	D	O	B
T	N	P	O	A
C	S	D	O	O
M	N	A	N	I
D	T	A	N	O
T	A	T	A	O
N	O	S	I	T
H	T	O	S	N

Figura 6.2

Si lo haces a mano el trabajo es bastante fácil, pues no tienes que reordenar las columnas en la red —simplemente las lees sin orden.

El desciframiento es también bastante fácil. Simplemente escribes las columnas en la red según indica la palabra clave y entonces el texto original se lee fila a fila, de arriba a abajo. Es simplemente invertir el proceso. Para realizar el desciframiento no necesitas saber el tamaño de la red, ya que puedes hallarla a partir de la longitud del criptograma y de la longitud de la palabra clave.

Paso 3 El texto cifrado se forma leyendo por columnas, de izquierda a derecha:

NEIIA	TCMDT	NHNLT	HINSN
TAOTC	AOADP	DAATS	OAHRH
OOONN	AISUN	SABAO	IOOTN

Figura 6.3

Aquí tienes un criptograma que se ha hecho por transposiciones completas de columnas, con la palabra clave PERLA:

ANNOB SOZAE AAQRI RVOIC EOHZM
LRBSA SNSHS RUCNA

¿Quién dijo estas palabras? ¿En que ocasión?

¿Qué tal lo has pasado resolviendo este criptograma? Bien, querrás que la máquina lo haga por ti, ¿no? (si no es así, has tirado el dinero con este libro). Por tanto, aquí tienes el programa. Es capaz de cifrar y descifrar a partir de la palabra clave y la longitud del mensaje que introduces.

```
  10 REM COLUMNAS COMPLETAS
  20 PRINT "PROGRAMA DE CIFRADO
'COLUMNAS COMPLETAS'"
  30 PRINT AT 2,2;"MODO Y PALABR
A CLAVE"
  40 INPUT m$
  50 IF m$="0" THEN  GO TO 9999
  60 IF LEN m$<3 THEN  GO TO 80
  70 IF m$(1)="d" OR m$(1)="c" T
HEN  GO TO 100
  80 PRINT AT 2,0;"?"
  90 GO TO 40
 100 LET k$=m$(2 TO )
 105 PRINT AT 2,0;"MODO : ";m$(1
);" PALABRA CLAVE : ";k$
 107 LET cc=CODE "{"
 110 LET lk=LEN k$
 120 DIM k(lk)
 130 FOR i=1 TO lk
 140 LET b=cc
 160 FOR j=1 TO lk
 170 IF CODE k$(j)>=b THEN  GO T
O 200
 180 LET b=CODE k$(j)
 190 LET p=j
 200 NEXT j
 210 LET k$(p)="{"
 215 LET k(i)=p
 220 NEXT i
 230 PRINT AT 4,2;"TEXTO"
```

```
 240 INPUT t$
 250 FOR i=2 TO LEN t$
 260 IF i>=LEN t$ THEN  GO TO 30
0
 270 IF t$(i)<>" " THEN  GO TO 3
00
 280 LET t$=t$( TO i-1)+t$(i+1 T
O )
 290 GO TO 260
 300 NEXT i
 310 IF t$="0" THEN  GO TO 9999
 320 IF LEN t$>0 THEN  GO TO 350
 330 PRINT AT 4,0;"?"
 340 GO TO 240
 350 LET lt=LEN t$
 360 IF lt/lk=INT (lt/lk) THEN
GO TO 390
 370 LET t$=t$+"z"
 380 GO TO 350
 390 PRINT AT 4,0;"TEXTO : ";t$
 400 PRINT
 410 IF m$(1)="d" THEN  GO TO 48
0
 420 FOR i=1 TO lk
 430 FOR j=k(i) TO lt STEP lk
 440 PRINT t$(j);
 450 NEXT j
 460 NEXT i
 470 GO TO 9999
 480 DIM c$(lt)
 490 LET l=0
 500 FOR i=1 TO lk
 510 FOR j=k(i) TO lt STEP lk
 520 LET l=l+1
 530 LET c$(j)=t$(l)
 540 NEXT j
 550 NEXT i
 560 PRINT c$
9999 REM fin
```

Anotaciones para el programa de cifrado "columnas completas"

Líneas	
10-20	Comentario identificador del programa e impresión del título.
30-105	El programa pide el modo de operación (cifrar o descifrar) y la palabra clave que se usa para transponer las columnas. El programa termina si se introduce un "0"; si no es así, se examinan los datos y se da otra oportunidad de introducirlos si no son correctos; cuando no se produzca ningún error se imprimen.
107-220	Se calcula la matriz k, donde el elemento k(i) representa la posición en orden alfabético de la letra número i de k$, suponiendo que las letras de k$ estuvieran en orden alfabético.
230-340	Pide la introducción del texto, quita los espacios y salta al final del programa si texto = "0".
350-390	Si es necesario se añaden caracteres de relleno al texto, y se imprime éste en la pantalla.
400-460	Imprime el texto cifrado a partir del texto original introducido.
470	Salta al final del programa.
480-560	Coge el texto cifrado y lo imprime descifrado.
9999	Fin del programa.

Instrucciones de uso del programa de cifrado "columnas completas"

Este programa es capaz de cifrar y descifrar textos usando la transposición completa de columnas, según la palabra clave especificada por el usuario. Su uso es extremadamente simple.

El usuario introduce el modo y la palabra clave como una cadena única. La primera letra de la cadena debe ser "c" o "d", para indicar cifrar o descifrar, respectivamente. Debe haber, al menos, dos letras más siguiendo a esta primera letra. Estas letras representan la clave para la transposición.

Cuando se pide, se debe introducir el texto, bien sea para cifrarlo o para descifrarlo. Debe constar como mínimo de un carácter. El programa lo completará hasta alcanzar un múltiplo de la palabra clave, lo imprimirá y, a continuación, imprimirá también el texto cifrado o descifrado, según el modo de operación elegido.

En cualquier momento se puede salir del programa, introduciendo un "0". Al final del capítulo tienes algunos criptogramas de práctica.

Transposiciones de itinerario

Las transposiciones de columnas se han usado muy a menudo debido a que son muy sencillas de utilizar. El problema es, como veremos, que esta clave no es muy difícil de descifrar. La razón es que mezclar las columnas y sacar las filas no introduce suficiente aletoriedad. Un tipo diferente de transposición, llamada transposición de itinerario, consigue solucionar este problema.

Para las transposiciones de itinerario se usan unas pequeñas redes rectangulares y se escribe el texto original en ellas, siguiendo un camino concreto a lo largo de todas las celdas de la red. El texto cifrado se consigue sacando las letras de la red siguiendo una ruta distinta a como se escribieron. Estas dos rutas se llaman ruta de escritura y ruta de lectura, por razones obvias. El tamaño de la red, la ruta de lectura y la de escritura determinan el cifrado y son los factores necesarios para descifrar el texto.

```
AFKPU  UPKFA  EJOTY  YTOJE  ABCDE  UVWXY  EDCBA  YXWVU
BGLQV  VQLGB  DINSX  XSNID  FGHIJ  PQRST  JIHGF  TSRQP
CHMRW  WRMHC  CHMRW  WRMHC  KLMNO  KLMNO  ONMLK  ONMLK
DINSX  XSNID  BGLQV  VQLGB  PQRST  FGHIJ  TSRQP  JIHGF
EJOTY  YTOJE  AFKPU  UPKFA  UVWXY  ABCDE  YXWVU  EDCBA

OSVXY  OJFCA  ACFJO  YXVSO  KPTWY  KGDBA  ABDGK  YWTPK
JNRUW  SNIEB  BEINS  WURNJ  GLQUX  PLHEC  CEHLP  XUQLG
FIMQT  VRMHD  DHMRV  TQMIF  DHMRV  TQMIF  FIMQT  VRMHD
CEHLP  XUQLG  GLQUX  PLHEC  BEINS  WURNJ  JNRUW  SNIEB
ABDGK  YWTPK  KPTWY  KGDBA  ACFJO  YXVSO  OSVXY  OJFCA

EFOPY  YPOFE  AJKTU  UTKJA  ABCDE  UVWXY  EDCBA  YXWVU
DGNQX  XQNGD  BILSV  VSLIB  JIHGF  TSRQP  FGHIJ  PQRST
CHMRW  WRMHC  CHMRW  WRMHC  KLMNO  KLMNO  ONMLK  ONMLK
BILSV  VSLIB  DGNQX  XQNGD  TSRQP  JIHGF  PQRST  FGHIJ
AJKTU  UTKJA  EFOPY  YPOFE  UVWXY  ABCDE  YXWVU  EDCBA

ABFGO  YXTSK  ACDJK  YWVPO  OPVWY  KJDCA  KSTXY  OGFBA
CEHNP  WURLJ  BEILS  XUQNG  GNQUX  SLIEB  JLRUW  PNHEC
DIMQV  VQMID  FHMRT  TRMHF  FHMRT  TRMHF  DIMQV  VQMID
JLRUW  PNHEC  GNQUX  SLIEB  BEILS  XUQNG  CEHNP  WURLJ
KSTXY  OGFBA  OPVWY  KJDCA  ACDJK  YWVPO  ABFGO  YXTSK
```

Figura 6.4. Treinta y dos rutas diferentes para redes de 5 x 5. Siguiendo el alfabeto en orden normal aparece la ruta de escritura

También puedes modificar esta transposición empezando en una posición de la ruta que no sea la primera. Con este sistema tienes una ruta de escritura y una posición inicial de escritura, y una ruta de lectura y una posición inicial de lectura. Así se pueden producir textos cifrados muy interesantes.

Normalmente se usan redes de pequeño tamaño (de 5 × 5 a 8 × 8). Las posiciones que no se utilizan de la última red se rellenan con caracteres que no afecten al sentido del mensaje. El diagrama de la figura 6.4 muestra diferentes tipos de rutas en una red de 5 × 5.

Si interceptas un mensaje que ha sido cifrado con una transposición de itinerario, la resolución puede ser muy difícil. Tienes que probar tamaños de bloques y rutas hasta que encuentres las adecuadas. Hacer esto a mano, o incluso usando un pequeño ordenador, puede ser muy tedioso. Sin embargo, las transposiciones de itinerario no son muy seguras actualmente, ya que en un criptograma de cualquier tamaño se pueden eliminar un gran número de rutas posibles por medio de un análisis de frecuencia en varios bloques a la vez. Teniendo esta posibilidad en tu ordenador este problema se puede resolver con un tiempo razonable.

El siguiente programa lo puedes usar en tu ordenador personal para cifrar y descifrar mensajes por transposición de itinerario. Trabaja con redes de 5 × 5.

```
  10 REM TRANSPOSICION DE
         ITINERARIO
  20 DIM l$(50,25)
  30 FOR r=1 TO 32
  40 READ l$(r)
  50 NEXT r
  60 DATA "afkpubglqvchmrwdinsxe
joty"
  70 DATA "upkfavqlgbwrmhcxsnidy
toje"
  80 DATA "ejotydinsxchmrwbglqva
fkpu"
  90 DATA "ytojexsnidwrmhcvqlgbu
pkfa"
 100 DATA "abcdefghijklmnopqrstu
vwxy"
 110 DATA "uvwxypqrstklmnofghija
bcde"
 120 DATA "edcbajihgfonmlktsrqpy
xwvu"
```

```
 130 DATA "ywxvutsrqponmlkjihgfe
dcba"
 140 DATA "osvxyjnruwfimqtcehlpa
bdgk"
 150 DATA "ojfcasniebvrmhdxuqlgy
wtpk"
 160 DATA "acfjobeinsdhmrvglquxk
ptwy"
 170 DATA "yxvsowurnjtqmifplheck
gdba"
 180 DATA "kptwyglquxdhmrvbeinsa
cfjo"
 190 DATA "kgdbaplhectqmifwurnjy
xvso"
 200 DATA "abdgkcehlpfimqtjnruwo
svxy"
 210 DATA "ywtpkxuqlgvrmhdsniebo
jfca"
 220 DATA "efopydgnqxchmrwbilsva
jktu"
 230 DATA "ypofexqngdwrmhcvslibu
tkja"
 240 DATA "ajktubilsvchmrwdgnqxe
fopy"
 250 DATA "utkjavslibwrmhcxqngdy
pofe"
 260 DATA "abcdejihgfklmnotsrqpu
vwxy"
 270 DATA "uvwxytsrqpklmnojihgfa
bcde"
 280 DATA "edcbafghijonmlkpqrsty
xwvu"
 290 DATA "yxwvupqrstonmlkfghije
dcba"
 300 DATA "abfgocehnpdimqvjlruwk
stxy"
 310 DATA "yxtskwurljvqmidpnheco
gfba"
 320 DATA "acdjkbeilsfhmrtgnquxo
pvwy"
 330 DATA "ywvpoxuqngtrmhfsliebk
jdca"
 340 DATA "opvwygnquxfhmrtbeilsa
cdjk"
```

```
 350 DATA "kjdcasliebtrmhfxuqngy
wvpo"
 360 DATA "kstxyjlruwdimqvcehnpa
bfgo"
 370 DATA "ogfbapnhecvqmidwurljy
xtsk"
 375 DEF FN a()=22701+x+32*y
 377 LET ca=CODE "a"-1
 380 CLS
 390 PRINT "TRANSPOSICION DE ITI
NERARIO"
 400 PRINT AT 2,2;"MODO (NUMERO
CLAVE)"
 410 INPUT m$
 420 IF m$="0" THEN  GO TO 9999
 430 IF m$="1" THEN  GO TO 1010
 440 IF m$="s" THEN  GO TO 1510
 450 LET lm=LEN m$
 460 IF lm<2 THEN  GO TO 520
 470 IF m$(1)<"c" OR m$(1)>"d" T
HEN  GO TO 520
 480 FOR i=2 TO lm
 490 IF m$(i)<"0" OR m$(i)>"9" T
HEN  GO TO 520
 500 NEXT i
 510 GO TO 540
 520 PRINT AT 2,0;"?"
 530 GO TO 410
 540 LET k=VAL m$(2 TO )
 550 IF k<1 OR k>=r THEN  GO TO
520
 560 PRINT AT 2,0;"MODO : ";m$(1
);" NUMERO CLAVE : ";k
 561 PRINT AT 4,0;"ITINERARIO :"
 562 FOR y=0 TO 4
 563 PRINT AT 4+y,13;l$(k)(y*5+1
 TO y*5+5)
 564 NEXT y
 565 PLOT 100,100
 566 DRAW 0,45
 567 DRAW 46,0
 568 DRAW 0,-45
 569 DRAW -46,0
 570 PRINT AT 10,2;"TEXTO"
```

```
 580 INPUT t$
 590 FOR i=1 TO LEN t$
 600 IF i>LEN t$ THEN  GO TO 670
 610 IF t$(i)<>" " THEN  GO TO 6
70
 620 LET r$=""
 630 IF i>1 THEN  LET r$=t$( TO
i-1)
 640 IF i<LEN t$ THEN  LET r$=r$
+t$(i+1 TO )
 650 LET t$=r$
 660 GO TO 600
 670 NEXT i
 680 IF t$="0" THEN  GO TO 9999
 690 LET lt=LEN t$
 700 IF lt>0 THEN  GO TO 730
 710 PRINT AT 10,0;"?"
 720 GO TO 580
 730 IF lt/25=INT (lt/25) THEN
GO TO 770
 740 LET t$=t$+"z"
 750 LET lt=lt+1
 760 GO TO 730
 770 PRINT AT 10,0;"TEXTO : ";t$
 780 PRINT
 790 IF m$(1)="d" THEN  GO TO 91
0
 800 DIM c$(25)
 810 FOR i=1 TO 25
 820 FOR j=1 TO 25
 830 IF l$(k,j)=CHR$ (ca+i) THEN
  LET c$(j)=t$(i)
 840 NEXT j
 850 NEXT i
 860 PRINT c$;
 870 IF lt=25 THEN  GO TO 9999
 880 LET t$=t$(26 TO )
 890 LET lt=lt-25
 900 GO TO 800
 910 DIM c$(25)
 920 FOR i=1 TO 25
 930 FOR j=1 TO 25
 940 IF l$(k,j)=CHR$ (ca+i) THEN
  LET c$(i)=t$(j)
```

```
 950 NEXT j
 960 NEXT i
 970 PRINT c$;
 975 IF lt=25 THEN  GO TO 9999
 980 LET t$=t$(26 TO )
 990 LET lt=lt-25
1000 GO TO 910
1010 IF r<=50 THEN  GO TO 1070
1020 PRINT AT 2,0;"?"
1030 PRINT AT 4,0;"LIBRERIA COMP
LETA"
1040 BEEP 1,0
1050 PRINT AT 4,0;TAB 13
1060 GO TO 410
1070 PRINT AT 2,0;"NUMERO DE ITI
NERARIO : ";r;" "
1080 PLOT 100,92
1090 DRAW 0,48
1100 DRAW 48,0
1110 DRAW 0,-48
1120 DRAW -48,0
1130 LET x=0
1140 LET y=0
1150 POKE FN a(),184
1160 LET r$=INKEY$
1170 IF r$="" THEN  GO TO 1160
1180 POKE FN a(),56
1185 IF r$="0" THEN  GO TO 9999
1190 IF r$=CHR$ 13 THEN  GO TO 1
320
1200 IF r$="8" AND x+y<8 THEN  G
O TO 1290
1210 IF r$<>"5" OR x+y=0 THEN  G
O TO 1250
1220 LET x=x-1
1230 IF x<0 THEN  LET x=4: LET y
=y-1
1240 GO TO 1150
1250 IF r$="6" AND y<4 THEN  LET
 y=y+1: GO TO 1150
1260 IF r$="7" AND y>0 THEN  LET
 y=y-1: GO TO 1150
1270 IF (r$<"a" OR r$>"y") AND r
$<>" " THEN  BEEP .25,12: GO TO
```

```
1150
1280 PRINT AT 5+y,13+x;r$
1290 LET x=x+1
1300 IF x>4 THEN  LET x=0: IF y<
4 THEN  LET y=y+1
1310 GO TO 1150
1320 DIM c$(25)
1330 FOR y=0 TO 4
1340 FOR x=0 TO 4
1350 LET r$=SCREEN$ (5+y,13+x)
1360 IF r$<>" " THEN  GO TO 1400
1370 POKE FN a(),23
1380 BEEP 1,0
1390 GO TO 1130
1400 LET c=CODE r$-ca
1410 IF c$(c)=r$ THEN  GO TO 137
0
1420 LET c$(c)=r$
1430 NEXT x
1440 NEXT y
1450 FOR y=0 TO 4
1460 FOR x=0 TO 4
1470 LET l$(r,y*5+x+1)=SCREEN$ (
5+y,13+x)
1480 NEXT x
1490 NEXT y
1495 LET r=r+1
1500 GO TO 380
1510 PRINT AT 2,2;"NOMBRE";TAB 1
8
1520 INPUT r$
1525 PRINT AT 2,0;"NOMBRE : ";r$
1530 SAVE r$ LINE 380
1540 GO TO 380
9999 REM fin
```

Anotaciones para el programa de cifrado "transposición de itinerario"

Líneas

10 Comentario identificador del programa.

20-50 Lectura de las "rutas estándar".

Líneas

60-370	Sentencias DATA que contienen 32 alfabetos, de 25 letras, escritos siguiendo rutas estándar.
377-390	Inicialización del programa e impresión del título.
400-560	Se pide la introducción del modo y la clave; si es "0" se termina el programa; si es "1" el usuario puede crear otra ruta para la librería de rutas estándar; si es "s" el usuario puede salvar el programa incluyendo la librería de rutas. Si no es ninguno de los casos anteriores, el modo debe ser "c" o "d", seguido del número de ruta requerido. Se comprueban los datos introducidos y, cuando son correctos, se imprimen.
561-569	Se imprime en la pantalla la ruta, con una caja dibujada alrededor.
570-780	Pide la introducción del texto y lo lee; quita los espacios; si es "0" se termina el programa; si no hay ningún carácter distinto de espacio es necesario volver a leer el texto. El texto se rellena hasta alcanzar una longitud múltiplo de 25 y se imprime por pantalla.
790	Decide entre cifrado o descifrado, según el modo.
800-900	El bucle va imprimiendo los bloques transpuestos del texto original de 25 en 25 caracteres; termina con el último bloque (línea 870).
910-1000	El bucle va imprimiendo los bloques transpuestos del texto cifrado de 25 en 25 caracteres; termina con el último bloque (línea 975).
1010-1500	Rutina para actualizar la librería de rutas (las notas adjuntas dan más detalles).
1070-1180	Dibuja una caja y lee una tecla del usuario.
1185-1310	Si la tecla introducida es "0" se termina; si es →, ←, ↑, ↓, el cursor se mueve en la dirección correspondiente; si es un carácter comprueba que está entre la "a" y la "y" (si no está en este rango avisa con un pitido); el bucle retorna para aceptar la siguiente tecla. Cuando se sale de la rutina ya tenemos una nueva ruta creada.
1320-1500	Operaciones con la ruta en el área de pantalla de la memoria del ordenador.
1510-1540	Pregunta el nombre con el que se va a salvar el programa con la nueva librería, lee el nombre, lo imprime y salva en cinta. Vuelve a la línea 390, tras limpiar la pantalla en la línea 380.
9999	Línea de fin de programa.

Instrucciones de uso para el programa de cifrado "transposición de itinerario"

Como es ya habitual, el programa necesita la introducción del modo y del número clave. Como siempre, el modo es "c" o "d" y el número clave selecciona una de las rutas de librería almacenadas en el programa. El número clave debe estar entre 1 y 50.

El modo y la ruta se imprimen en la pantalla. Si la ruta está formada únicamente por espacios, quiere decir que no existe ninguna ruta correspondiente al número clave elegido. En este caso es necesario terminar el programa con un "0" y volver a empezar.

Se lee y se escribe el texto, seguido por el texto cifrado o descifrado. El texto leído se rellena hasta alcanzar una longitud múltiplo de 25 y los caracteres de relleno ("Z") se incluyen en la transposición.

Cuando el ordenador pide el modo y el número clave también se puede introducir una "l" o una "s". La "l" permite al usuario crear una nueva ruta en la pantalla, por medio de las teclas de cursor →, ←, ↑ o ↓. Se dibuja una rejilla y el usuario pone caracteres en la rejilla para formar la ruta. La ruta queda determinada según el orden alfabético de las letras de la rejilla. Para llenar la rejilla hay que introducir letras de la "a" a la "y".

La opción "s" permite salvar el programa y su librería de rutas. Sirve para salvar una ruta creada con la opción "l". El programa dispone, en principio, de 32 rutas estándar. La matriz de la librería puede llegar a tener hasta 50 (o más, si modificas tú mismo el programa).

El programa también se puede utilizar para ayudarte a analizar textos cifrados. Verás que si pruebas unas cuantas rutas en un texto cifrado, aparecen fragmentos del texto original. Con esto puedes fácilmente determinar la naturaleza de la ruta que se usó para cifrar y puedes seleccionar o crear una ruta adecuada para su resolución.

Cifrados por giro de rejilla

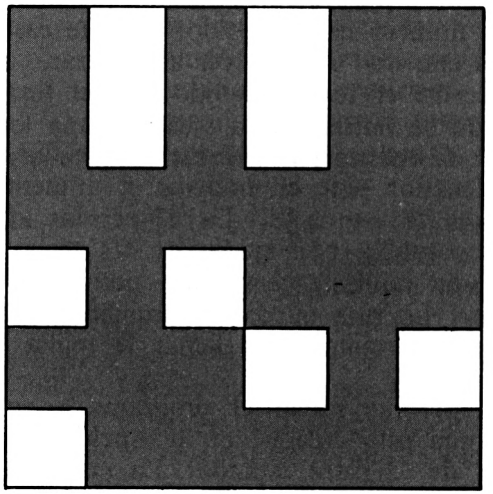
El último tipo de cifrado de este capítulo se le ocurrió, en primer lugar, a un caballero llamado Cardano en el Renacimiento. Originalmente se hacía uso de una rejilla cuadrada con un número par de celdas. Había que trazar líneas horizontales y verticales para dividir la rejilla en cuatro partes iguales. A continuación, se recortan un número de cuadrados igual a un cuarto del número total de cuadrados de la rejilla. Estos cuadrados se eligen de forma que estén distribuidos por cada una de las cuatro partes y con la condición de que los cuadrados de una parte no se solapen con los de otra si la rejilla rota sobre su centro.

Esta tarjeta que ha resultado se coloca en el papel y se escribe el mensaje, letra a letra, en los cuadrados recortados hasta que estén todos

llenos. A continuación, se hace girar la tarjeta, o rejilla, noventa grados para que aparezcan partes del papel sin escribir, y poder poner letras sobre estas posiciones. Cuando la rejilla ha rotado cuatro veces empiezas un nuevo bloque y continúas con este sistema hasta que el mensaje esté completo (rellenándolo con letras adicionales si es necesario).

Aquí tienes un ejemplo para que veas cómo funciona:

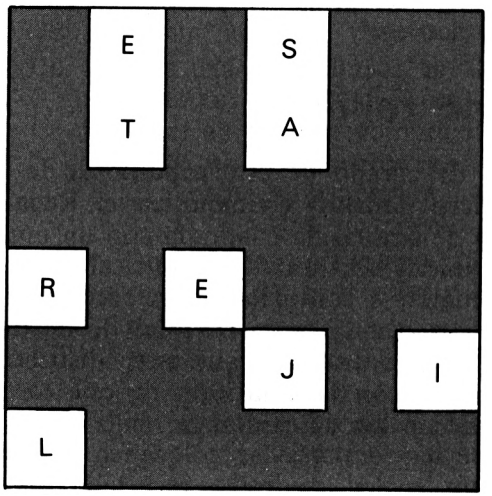
Rejilla modelo



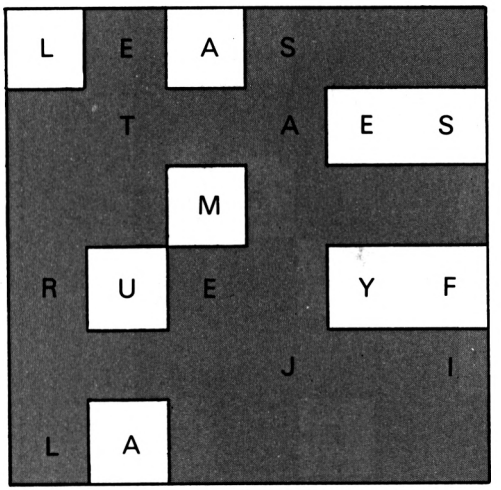
Mensaje

ESTA REJILLA ES MUY
FACIL DE UTILIZAR
(31 letras)

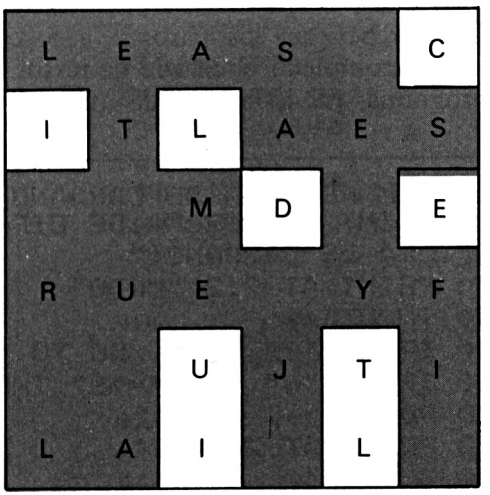
Paso 1: Se escriben las primeras nueve letras:



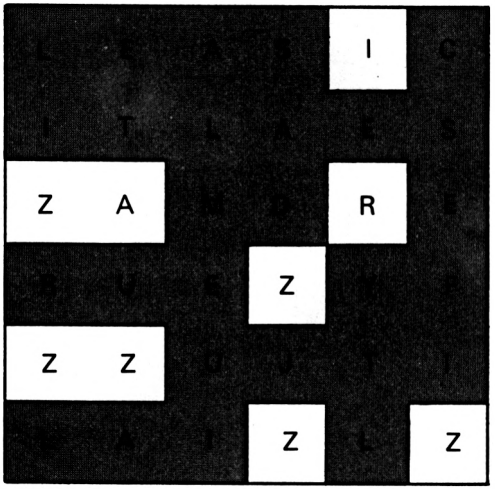
Paso 2: Se escriben las segundas nueve letras:



Paso 3: Se escriben las terceras nueve letras:



Paso 4: En los huecos que quedan se pone la letra Z:



Paso 5: El texto cifrado resulta de leer las letras fila a fila:

LEASIC ITLAES ZAMDRE RUEZYF ZZUJTI LAIZLZ

A continuación se repetirían los pasos 1 a 5, cogiendo bloques de 36 letras cada vez, para completar el cifrado de textos de mayor extensión.

Aquí está el programa que lo hace todo automáticamente:

```
  10 REM REJILLA DE CARDANO
  20 PRINT "PROGRAMA DE CIFRADO
'REJILLA DE CARDANO'"
  30 PRINT AT 2,2;"MODO"
  40 INPUT m$
  50 IF m$="0" THEN  GO TO 9999
  60 IF m$="d" OR m$="c" THEN  G
O TO 90
  70 PRINT AT 2,0;"?"
  80 GO TO 40
  90 PRINT AT 2,0;"MODO : ";m$
  93 DIM g(6,6)
  97 LET nh=0
 100 PLOT 188,92
 110 DRAW 0,64
 120 DRAW 64,0
```

```
 130 DRAW 0,-64
 140 DRAW -64,0
 150 PLOT 220,92
 160 DRAW 0,64
 170 PLOT 188,124
 180 DRAW 64,0
 190 FOR q=1 TO 4
 200 LET sx=24
 210 IF q=2 OR q=3 THEN  LET sx=
28
 220 LET sy=3
 230 IF q>2 THEN  LET sy=7
 240 PRINT AT sy,sx;"123";AT sy+
1,sx;"456";AT sy+2,sx;"789"
 250 PRINT AT 4,0;"CUADRANTE ";q
;" AGUJERO ?"
 260 PRINT AT 4,19;" ";CHR$ 8;
 270 LET r$=INKEY$
 280 IF r$="" THEN  GO TO 270
 290 IF r$="0" THEN  GO TO 9999
 300 IF r$="n" THEN  GO TO 620
 310 IF r$>="1" AND r$<="9" THEN
  GO TO 350
 320 PRINT AT 4,18;"?"
 330 BEEP 1,0
 340 GO TO 260
 350 LET v=VAL r$
 360 PRINT v
 370 LET gy=INT ((v-1)/3)+1
 380 LET gx=v-3*(gy-1)
 390 IF q=2 OR q=3 THEN  LET gx=
gx+3
 400 IF q>2 THEN  LET gy=gy+3
 410 IF g(gy,gx)=1 THEN  GO TO 3
30
 420 FOR y=1 TO 6
 430 FOR x=1 TO 6
 440 IF g(y,x)=0 THEN  GO TO 530
 450 LET yy=y
 460 LET xx=x
 470 FOR r=1 TO q-1
 480 LET i=yy
 490 LET yy=xx
 500 LET xx=7-i
```

```
 510 IF yy=gy AND xx=gx THEN  GO
 TO 330
 520 NEXT r
 530 NEXT x
 540 NEXT y
 550 LET g(gy,gx)=1
 560 IF gx>3 THEN  LET gx=gx+1
 570 IF gy>3 THEN  LET gy=gy+1
 580 PRINT AT 2+gy,23+gx;" "
 590 LET nh=nh+1
 600 IF nh<9 THEN  GO TO 260
 610 LET q=4
 620 IF q=4 AND nh<9 THEN  GO TO
 320
 630 FOR i=0 TO 2
 640 FOR j=0 TO 2
 650 IF CODE SCREEN$ (sy+i,sx+j)
<>32 THEN  PRINT AT sy+i,sx+j;"
"
 660 NEXT j
 670 NEXT i
 680 NEXT q
 690 PRINT AT 4,0;TAB 19
 700 PRINT AT 12,2;"TEXTO"
 710 INPUT t$
 720 FOR i=1 TO LEN t$
 730 IF i>LEN t$ THEN  GO TO 800
 740 IF t$(i)<>" " THEN  GO TO 8
00
 750 LET r$=""
 760 IF i>1 THEN  LET r$=t$( TO
i-1)
 770 IF i<LEN t$ THEN  LET r$=r$
+t$(i+1 TO )
 780 LET t$=r$
 790 GO TO 730
 800 NEXT i
 810 IF t$="0" THEN  GO TO 9999
 820 LET lt=LEN t$
 830 IF lt/36=INT (lt/36) THEN
GO TO 870
 840 LET t$=t$+"z"
 850 LET lt=lt+1
 860 GO TO 830
```

```
 870 PRINT AT 12,0;"TEXTO : ";t$
 880 PRINT
 890 DIM c$(6,6)
 895 LET rf=1
 900 IF m$="d" THEN  GO TO 1110
 910 LET cn=0
 920 FOR q=1 TO 4
 930 FOR y=1 TO 6
 940 FOR x=1 TO 6
 950 IF g(y,x)=0 THEN  GO TO 980
 960 LET cn=cn+1
 970 LET c$(y,x)=t$(cn)
 980 NEXT x
 990 NEXT y
1000 GO SUB 2000
1010 NEXT q
1020 FOR y=1 TO 6
1030 FOR x=1 TO 6
1040 PRINT c$(y,x);
1050 NEXT x
1060 NEXT y
1070 IF lt=36 THEN  GO TO 9999
1080 LET t$=t$(37 TO )
1090 LET lt=lt-36
1100 GO TO 910
1110 LET cn=0
1120 FOR y=1 TO 6
1130 FOR x=1 TO 6
1140 LET cn=cn+1
1150 LET c$(y,x)=t$(cn)
1160 NEXT x
1170 NEXT y
1180 FOR q=1 TO 4
1190 FOR y=1 TO 6
1200 FOR x=1 TO 6
1210 IF g(y,x)>0 THEN  PRINT c$(
y,x);
1220 NEXT x
1230 NEXT y
1240 GO SUB 2000
1250 NEXT q
1260 IF lt=36 THEN  GO TO 9999
1270 LET t$=t$(37 TO )
1280 LET lt=lt-36
```

```
1290 GO TO 1110
2000 FOR y=1 TO 6
2010 FOR x=1 TO 6
2020 IF g(y,x)<>rf THEN  GO TO 2
070
2030 LET g(y,x)=0
2040 LET yy=x
2050 LET xx=7-y
2060 LET g(yy,xx)=3-rf
2070 NEXT x
2080 NEXT y
2090 LET rf=3-rf
2100 RETURN
9999 REM fin
```

Programa "Rejilla de Cardano". Anotaciones

Líneas	
10-20	Comentario identificador del programa e impresión del título.
30-90	Pide la introducción del modo; si es "0" el programa termina; el modo debe ser "c" o "d"; vuelve a pedir la introducción del dato hasta que éste sea aceptable, y entonces lo imprime en la pantalla.
93-180	Dibuja la rejilla inicial para especificar la posición de los agujeros.
190-690	Rutina para leer la posición de los agujeros de la rejilla (mira las notas que se acompañan).
200-250	Pide al usuario que especifique qué posiciones quiere agujerear.
260-340	Lee la tecla pulsada; si es "0" termina; si es "n" se sale de este cuadrante; si no es ninguna de las anteriores, la tecla debe ser un número entre "1" y "9", que especifica la posición de un agujero. La rutina repite este ciclo hasta que se pulsa una tecla correcta.
350-680	La rutina comprueba que la posición del agujero no sea incompatible (es decir, no coincida) con los agujeros de otros cuadrantes al hacerlos rotar. Si se detecta un error suena una alarma y hay que volver a introducir el dato. También se asegura de que se especifican exactamente nueve agujeros.

Líneas	
690-880	Pide la introducción del texto, quita los espacios y si es "0" termina. Rellena el texto hasta que alcanza una longitud múltiplo de 36 y lo imprime por pantalla.
890-900	Empieza el proceso de cifrado y selecciona entre cifrado y descifrado según el modo.
910-1010	Cifra un cuadrante y hace rotar la rejilla para poner los siguientes caracteres.
1020-1060	Imprime un bloque de 36 caracteres.
1070-1100	Se prepara a hacer el siguiente bloque de 36 caracteres, si existe; termina (línea 1070) si ya no quedan.
1110-1170	Coge el siguiente grupo de 36 caracteres en un bloque.
1180-1290	Descifra cuadrante a cuadrante haciendo rotar la máscara según va siendo necesario.
2000-2100	Subrutina para simular la rotación de la rejilla.
9999	Línea de fin de programa.

Instrucciones de uso del programa de cifrado "Rejilla de Cardano"

El programa empieza pidiendo el modo de operación. Hay que introducir "c" para cifrar y "d" para descifrar. Se comprueba el dato y hay que volver a introducirlo si hay algún error.

El usuario debe entonces especificar la rejilla que se va a usar. Esto se hace en la pantalla. Se imprime una rejilla con los números 1-9 en el cuadrante de arriba, a la izquierda. El usuario introduce un número entre 1 y 9 para indicar que esa posición de la rejilla tiene un agujero. Este proceso se repite cuadrante a cuadrante hasta que se han especificado nueve agujeros. Si en cualquier momento un agujero de un cuadrante coincide con otro de otro cuadrante si se hace rotar este último, se avisa del error con un pitido y hay que seleccionar otro agujero.

Una vez está terminada la rejilla, el programa lee e imprime el texto. Se le completa hasta alcanzar una longitud múltiplo de 36 y se imprime el texto resultante de aplicar la transposición con la rejilla que antes se formó.

Como siempre, se sale del programa tecleando "0".

El criptoanálisis de cifrados de rejilla no es muy complicado. El tamaño del espacio de las claves está limitado por el tamaño de la rejilla y por el hecho de que no hay muchas posibilidades de elegir los cuadrados. También la rotación natural del método hace que sea posible utilizar métodos especiales para solucionar más fácilmente el problema.

Otros cifrados por transposición

Se pueden usar muchos otros tipos de transposición. Es bastante fácil escribir programas para ellos. La razón de no incluir más transposiciones aquí, es que los expuestos son suficientemente sencillos para ser analizados por un ordenador personal. Además, con estos cifrados concretos es mucho más fácil describir el método general para descifrar la clave de todos los tipos de transposiciones. Estos métodos se discuten en el siguiente capítulo.

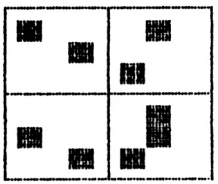
Probablemente es una buena idea asegurarte de que has comprendido la esencia de los métodos de transposición antes de intentar ver cómo forzar su protección. En concreto, intenta entender bien el tipo de mezcla o confusión que produce la transposición, introduciendo para ello el alfabeto normal como mensaje para ser cifrado. Haz los criptogramas de práctica porque, a no ser que comprendas bien todo, te será difícil entender las razones por las que funciona el método de análisis.

Criptogramas de práctica

Ejemplos de la rejilla de Cardano

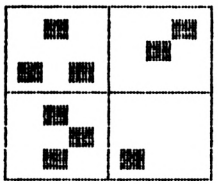
1. l i p a a c d s m e l o h e a u o s s p s e e e r a d u t e o n
e d r a e e u r s p n r c o z i u r z o e n d z l e s z a n o e
s c z a q u z u

Rejilla:



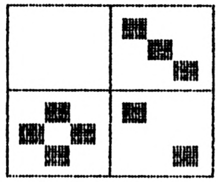
2. h c l n b u o o s e a i n d t e r m a a b g r u e e s e s n u m
e e n a n l o d m i e d s a n u t c e r s r a r a s s y o d s i e
n f t o e r e e z n s o e d c z a e e s r q a u z z e l z z z z
z z a z p z z s z p z o

Rejilla:



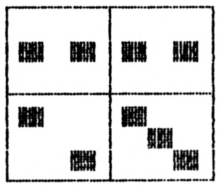
3. e s u l n n q a u m a e g e d r i s o m v u a i j d e n v v e r
e n a e c a c r o r m e o m i i y r e e n a z c e i n s o a n d
l o o d n s s e e e e a i s z l z a i e n z m t z e m r p o r z r
e e q z n z o u s l z e

Rejilla:



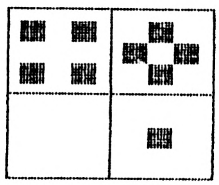
4. i n n c c a c a o n d f i a n d a o r e l e a l d m i c c e u s
u e s e e a p v e c n e t i i m r l r i o c i t h e a a o y m o
n f q l t a u o z z z z z z d z i g z e z z z z z z s z z t z z
z z z z i z z z o z z n

Rejilla:



5. u n n p a o a e g i r d e o a c u o s s e p v a r i e v n a r c
i e l u a a t u a m l s a n b a c r o b s r a t s a a n a d o o
t s s i i r e p n u i c m i e c i p n o r v t a a d e i n a e d
o s d g n r t e a l a q c z u l a a z z z n z t o z h z a z z z
z z z z z z z z b z z z z z z z

Rejilla:



6. Itinerario: 4

l i o i h s m s n a e u d a l d h a m n l n d u e s e e e e o b
s u u i o n p q b s e o s r r d n o e c o b s c e l r n e u s e
o r q o b s a s i o y z o s o a z t b t t z u a n e z l n e d z
o e l n

y t o j e
x s n i d
w r m h c
v q l g b
u p k f a

Ejemplo de transposición de ruta

7. Itinerario: 9

```
s e n t i i o b a a n m t e n s e i n d l o s t e d r z z z c e
e e z y n b c s r e u o e z a s n a
```

o	s	v	x	y
j	n	r	u	w
f	i	m	q	t
c	e	h	l	p
a	b	d	g	k

8. Itinerario: 23

```
u m a n u j e r d i e i s a r m p r e l d r e v a l a s d a v o
e n e o s a c l n a t u r n e m l a q e d e t u e l a v d a d r
e s e a a g b a d a r z z z e l z z z z z z z z z z z z z z z z
z z z z
```

e	d	c	b	a
f	g	h	i	j
o	n	m	l	k
p	q	r	s	t
y	x	w	v	u

9. Itinerario: 25

```
p a c a o r a b c s a a a a y r n n a c u o h a m i n s r e o a
e e m m c u p l t q e r a o z a z z
```

a	b	f	g	o
c	e	h	n	p
d	i	m	q	v
j	l	r	u	w
k	s	t	x	y

10. Itinerario: 15

```
e l u o n q e t e g n i n u e e i n s o n d e e x c e t u t p o
d i s s e n e t s o n i n e o e e y a s m a s e e n e s j t s o
e e t l n e a o m d i o d l i s e u v o o n e r q l r r u e o i
e r d e a z z z z z z z z z z z z z z z z z z z z z z z z z z z
```

a	b	d	g	k
c	e	h	l	p
f	i	m	q	t
j	n	r	u	w
o	s	v	x	y

Ejemplos de columnas completas

11. Palabra clave: corleone

```
eodpd eeama rmcio sdrbd aieli neacd
eyoce dnisd ragog raina sedin spare
rtela orsms nsrau sesss iidne canel
oditg tezel ocioi poran repta ossao
lrooi mntar oatos tiaua bepom irbte
slsif ivepo ouulo abrcg fnraa oftni
asman esnrn es
```

12. Palabra clave: materialismo

```
irdou nmoee eilis uncom usarr ttilr
brnrn aseel crfld sckut euahh ncete
eaaaa ueaaq ei
```

13. Palabra clave: perspicacia

```
sncva pfrns mttfr idana sdmbs oeong
ogaan oldsp eooae eolea uocuo utobi
iuaan suroa nrsmd miaex rverr anndl
hnudc asdec aerei jrvee zpues tduea
aisis eonfl spoda eiani qolka hnosl
tseae aelnn siosp irevs ugsge q
```

14. Palabra clave: aerobic

```
ureln pnprn aurne aeaoe rfepr ecoea
esenp regru eagoj aatlr lntas mdout
pcdug maodq aanrq af
```

15. Palabra clave: divorcio

```
osial yrrkc stson pesus aesee seded
nlooa znruc hmipw osoda rdrrd enuaa
garae nsenl eb
```

7
Cómo resolver las transposiciones

Los mensajes puestos en clave por medio de transposiciones son más difíciles de resolver que los que utilizaron sustituciones monoalfabéticas. Las transposiciones separan las palabras y destrozan los digramas y trigramas; luego, para resolver una transposición, tienes que probar diferentes reordenaciones hasta que los fragmentos de texto resulten aparentemente razonables.

A primera vista esto parece muy pesado, pero afortunadamente la mayoría de las transposiciones siguen un sistema, y esto se puede aprovechar en el criptoanálisis. Normalmente, un sistema de transposición tiene la propiedad de mezclar de la misma forma los distintos fragmentos del texto. Esto da al criptoanalista algo sobre lo que trabajar.

Por ejemplo, en las transposiciones de columnas con palabra clave, los trozos de texto consecutivos de la misma longitud que la palabra clave se reordenan de idéntica manera. Esto se puede usar para reducir el trabajo de buscar posibles reordenaciones, ya que una reordenación errónea que parezca buena en un trozo de texto no lo será en el siguiente, y quedará, por tanto, desechada. La idea es buscar una reordenación que haga que todos los bloques parezcan con significado. Este proceso se denomina de anagramas múltiples, y es el método general de resolución de transposiciones.

Veamos algunos ejemplos.

Resolución de transposiciones de columnas

Supongamos que el siguiente mensaje cae en nuestras manos:

LRBLR SNELO ASILR TSLVE AEAAB
AENEJ LVARI IIEAI LORAE IELQT

Lo primero es hallar de qué tamaño era el bloque de transposición. El criptograma tiene 50 letras. Los factores primos de 50 son dos y cinco, y los posibles tamaños del bloque son:

$2 \times 25, \quad 10 \times 5, \quad 5 \times 10, \quad 25 \times 2$

En este punto tenemos que hacer una suposición, y dar marcha atrás más tarde si descubrimos que es errónea. Un bloque muy largo y estrecho no sería lógico; por tanto, tendremos cinco filas y diez columnas o diez filas y cinco columnas. Supongamos que era de diez filas. El siguiente paso es escribir el criptograma por columnas en un bloque de este tamaño:

L	A	A	L	L
R	S	E	V	O
B	I	A	A	R
L	L	A	R	A
R	R	B	I	E
S	T	A	I	I
N	S	E	I	E
E	L	N	E	L
L	U	E	A	Q
O	E	J	I	T

Y ahora veamos si la suposición sobre el tamaño del bloque es razonable. Para ello hallamos el tanto por ciento de vocales en cada fila y en cada columna. Los resultados se muestran en la figura 7.1:

					Vocales en fila (por 100)
L	A	A	L	L	2/5 = 40
R	S	E	V	O	2/5 = 40
B	I	A	A	R	3/5 = 60
L	L	A	R	A	2/5 = 40
R	R	B	I	E	2/5 = 40
S	T	A	I	I	3/5 = 60
N	S	E	I	E	3/5 = 60
E	L	N	E	L	2/5 = 40
L	U	E	A	Q	3/5 = 60
O	E	J	I	T	3/5 = 60

Vocales en columnas (por 100): 2/10 = 20, 4/10 = 40, 7/10 = 70, 7/10 = 70, 5/10 = 50

Figura 7.1

En la tabla del apéndice de la frecuencia de las letras vemos que aproximadamente un 40 por 100 del texto deben ser vocales. Conseguimos este valor en cinco de las diez filas. Los valores de las columnas varían más, pero también se aproximan al 40 por 100. Esto nos indica que hemos elegido el bloque del tamaño adecuado. Si nos hubiéramos equivocado, el valor de 40 por 100 no se cumpliría como se nos cumple en este caso.

No resta más que reordenar las columnas de forma que en las filas se lea el texto original. No importa que las filas no contengan palabras completas o que haya palabras sin separación en medio de una fila. Simplemente se trata de reordenar las columnas de forma que cada fila sea razonable. Ahora es cuando la ciencia entra en acción. Para reordenar las columnas se pueden usar los datos de los digramas.

Toma una columna e intenta ver de un modo lógico qué columnas deben estar a su derecha y a su izquierda. ¿Cómo? Cogiendo la columna que contenga la más probable letra de contacto hacia la derecha y hacia la izquierda.

Los artículos en castellano son palabras que suelen aportar muchos datos, pero en este caso tenemos mala suerte, ya que tanto en las filas 1, 4, como en la 8, puede haber artículos, pero se encuentran enmascarados por la repetición de las letras A y L y L y E, por lo que no podemos sacar ninguna información.

La clave para descifrar nuestro criptograma se encuentra en la línea nueve. Hay una "Q"; y las "Q", en castellano, siempre van seguidas de una "U", ya tenemos dos columnas colocadas. La probabilidad de que la "E" sigue a la "U" para formar "QUE" es muy alta, pero al ordenar las columnas para formar esta palabra no obtenemos ningún resultado. Otra solución, menos probable y que resulta ser la acertada, consiste en juntar la QU con la I de la siguiente fila. Sólo nos quedan dos columnas por colocar, y eso es fácil: basta con probar.

Por tanto, la solución es:

4 3 1 5 2

Si reordenas según estos números la tabla, leerás la posible forma de abrir una puerta secreta de un castillo.

Antes de la era de los ordenadores este trabajo era muy tedioso. La gente solía recortar los trozos de textos para poder ponerlos en distinto orden y ver si significaban algo. Pero con un ordenador este proceso se puede automatizar, ya que las estadísticas nos indican cuáles son las posiciones más posibles para cada columna.

El siguiente programa hace todo esto. Te invita a que supongas el tamaño del bloque y hace unos pequeños cálculos para ver si es el adecuado. A continuación, te pide que elijas una columna para empezar y él calcula las columnas que aparentemente deberían ir a su izquierda y a su derecha.

```
  10 REM ANALISIS POR COLUMNAS
              COMPLETAS
  20 PRINT AT 11,4;"PONGA LA CIN
TA CON DATOS";AT 12,3;"PULSE LUE
GO CUALQUIER TECLA"
  30 BEEP 1,12
  40 IF INKEY$="" THEN  GO TO 40
  50 LOAD "" DATA e()
  60 LOAD "" DATA t()
  70 CLS
  80 PRINT "ANALISIS POR COLUMNA
S COMPLETAS"
  90 PRINT AT 2,2;"TEXTO"
 100 INPUT t$
 110 FOR i=1 TO LEN t$
 120 IF i>LEN t$ THEN  GO TO 190
 125 IF t$(i)>="A" AND t$(i)<="Z
" THEN  LET t$(i)=CHR$ (CODE t$(
i)+CODE "a"-CODE "A")
 130 IF t$(i)<>" " THEN  GO TO 1
90
 140 LET r$=""
 150 IF i>1 THEN  LET r$=t$( TO
i-1)
 160 IF i<LEN t$ THEN  LET r$=r$
+t$(i+1 TO )
 170 LET t$=r$
 180 GO TO 120
 190 NEXT i
 200 IF t$="0" THEN  GO TO 9999
 210 LET lt=LEN t$
 220 IF lt>0 THEN  GO TO 250
 230 PRINT AT 2,0;"?"
 240 GO TO 100
 250 LET nf=0
 260 FOR i=2 TO INT (lt/2)
 270 IF lt/i=INT (lt/i) THEN  LE
T nf=nf+1
 280 NEXT i
 290 IF nf=0 THEN  GO TO 230
 300 DIM c(nf)
 310 DIM r(nf)
 320 LET nf=0
 330 FOR i=2 TO INT (lt/2)
```

```
 340 IF lt/i>INT (lt/i) THEN  GO
 TO 380
 350 LET nf=nf+1
 360 LET c(nf)=i
 370 LET r(nf)=lt/i
 380 NEXT i
 385 LET ca=CODE "a"-1
 390 PRINT AT 2,0;"TEXTO : ";t$
 400 PRINT
 410 PRINT "HAY ";nf;" MODOS POS
IBLES DE FACTORIZACION"
 420 PRINT
 430 FOR i=1 TO nf
 440 PRINT  INVERSE 1;i; INVERSE
 0;": ";r(i);" filas, ";c(i);" c
olumnas."
 445 NEXT i
 450 PRINT
 460 PRINT "DISTRIBUCION DE VOCA
LES? (S/N/0)"
 475 BEEP .5,8
 480 LET r$=INKEY$
 490 IF r$="" THEN  GO TO 480
 495 IF r$="n" THEN  GO TO 650
 500 IF r$="0" THEN  GO TO 9999
 505 IF r$="c" THEN  COPY : CLS
: GO TO 450
 515 CLS
 520 FOR i=1 TO nf
 530 PRINT  INVERSE 1;i; INVERSE
 0;": ";c(i);"x";r(i);" : ";
 540 FOR j=1 TO r(i)
 550 LET nv=0
 560 FOR k=1 TO c(i)
 570 LET r$=t$((k-1)*r(i)+j)
 580 IF r$="a" OR r$="e"  OR r$=
"i" OR r$="o" OR r$="u" THEN  LE
T nv=nv+1
 590 NEXT k
 600 PRINT INT (nv/c(i)*100);"%"
;
 610 NEXT j
 620 PRINT
 630 PRINT
```

```
 640 NEXT i
 650 PRINT
 660 INPUT "NUMERO DEL BLOQUE DE
 DIMENSIONES ?"; LINE r$
 663 IF r$="c" THEN  COPY : GO T
O 660
 665 LET bd=VAL r$
 667 IF bd=0 THEN  GO TO 9999
 670 IF bd<1 OR bd>nf OR bd>INT
bd THEN  GO TO 660
 680 LET nc=c(bd)
 690 LET nr=r(bd)
 691 DIM c$(nr,nc)
 692 FOR i=1 TO nr
 693 FOR j=1 TO nc
 694 LET c$(i,j)=t$((j-1)*nr+i)
 695 NEXT j
 696 NEXT i
 697 DIM b(nc)
 698 DIM f(nc)
 700 CLS
 710 FOR i=1 TO nc
 720 PRINT AT 0,i-1;INT (i/10);A
T 0,15+i;INT (i/10)
 730 PRINT AT 1,i-1;i-10*INT (i/
10);AT 1,15+i;i-10*INT (i/10)
 740 PRINT AT 2,i-1;"-";AT 2,15+
i;"-"
 750 NEXT i
 760 FOR i=1 TO nr
 770 PRINT c$(i)
 780 NEXT i
 790 GO SUB 8000
 810 LET f(cn)=1
 820 LET b(1)=cn
 830 GO SUB 8100
 840 PRINT AT 21,0;TAB 31;AT 21,
0;"PULSE b,c,d,i,l,n,p,r,s,w o 0
."
 850 LET r$=INKEY$
 860 IF r$="" THEN  GO TO 850
 865 PRINT AT 21,0;TAB 31
 867 IF r$="n" THEN  GO TO 697
 870 IF r$="b" THEN  CLS : GO TO
```

```
 390
 880 IF r$="c" THEN  COPY : GO T
O 840
 890 IF r$="0" THEN  GO TO 9999
 900 IF r$<>"1" AND r$<>"r" THEN
  GO TO 1160
 910 GO SUB 8050
 915 IF b(pc)=0 THEN  GO TO 910
 920 LET c=b(pc)
 930 GO SUB 8220
 970 PRINT AT sy,0;
 980 LET fc=32
 990 IF 22-sy>INT (nc/2) THEN  L
ET fc=6
1000 IF 22-sy>nc-1 THEN  LET fc=
13
1010 FOR i=1 TO nc
 892 IF i=c THEN  GO TO 1140
1030 PRINT i;
1050 PRINT ": ";
1060 LET p=0
1070 FOR j=1 TO nr
1080 LET cp=CODE c$(j,c)-ca
1090 LET tc=CODE c$(j,i)-ca
1100 IF r$="1" THEN  LET p=p+t(t
c,cp)
1110 IF r$="r" THEN  LET p=p+t(c
p,tc)
1120 NEXT j
1130 PRINT p;
1135 PRINT
1140 NEXT i
1151 INPUT "Pulse ENTER:"; LINE
r$
1152 GO SUB 8220
1153 GO TO 840
1160 IF r$<>"d" THEN  GO TO 1250
1170 GO SUB 8050
1175 IF b(pc)>0 THEN  LET f(b(pc
))=0: LET b(pc)=0
1180 FOR i=pc TO nc-1
1190 LET b(i)=b(i+1)
1200 IF b(i)>0 THEN  LET f(b(i))
=i
```

```
1210 NEXT i
1220 LET b(nc)=0
1230 GO SUB 8100
1240 GO TO 840
1250 IF r$<>"i" THEN  GO TO 1301
1255 GO SUB 8050
1257 IF b(nc)>0 THEN  LET f(b(nc
))=0
1259 IF pc>=nc THEN  GO TO 1290
1260 FOR i=nc TO pc+1 STEP -1
1270 LET b(i)=b(i-1)
1280 IF b(i)>0 THEN  LET f(b(i))
=i
1285 NEXT i
1292 LET b(pc)=0
1294 GO SUB 8100
1300 GO TO 840
1301 IF r$<>"w" THEN  GO TO 1310
1302 GO SUB 8050
1303 GO SUB 8000
1304 IF b(pc)>0 THEN  LET f(b(pc
))=0
1305 LET f(cn)=pc
1306 LET b(pc)=cn
1307 GO SUB 8100
1308 GO TO 840
1310 IF r$<>"p" THEN  GO TO 1319
1311 INPUT "Letras?";r$
1312 IF LEN r$<>2 THEN  GO TO 13
11
1313 LET l1=CODE r$( TO 1)-ca
1314 LET l2=CODE r$(2 TO )-ca
1315 IF l1<1 OR l1>26 OR l2<1 OR
 l2>26 THEN  GO TO 1311
1316 PRINT AT sy,0;"FREC: ";t(l1
,l2)
1318 GO TO 840
1319 IF r$="s" THEN  GO TO 1350
1320 PRINT AT 21,0;"?"
1330 BEEP 1,0
1340 GO TO 840
1350 CLS
1360 FOR j=1 TO nr
1365 FOR i=1 TO nc
```

```
1370 PRINT c$(j,b(i));
1380 NEXT i: NEXT j
1390 GO TO 9999
8000 INPUT "Que columna quiere p
oner?";cn
8010 LET cn=INT cn
8020 IF cn=0 THEN  GO TO 9999
8030 IF cn<1 OR cn>nc THEN  GO T
O 8000
8035 IF f(cn)>0 THEN  GO TO 8000
8040 RETURN
8050 INPUT "En que posicion?";pc
8060 LET pc=INT pc
8070 IF pc=0 THEN  GO TO 9999
8080 IF pc<1 OR pc>nc THEN  GO T
O 8050
8090 RETURN
8100 DIM p$(nr,nc)
8110 FOR i=1 TO nc
8115 PRINT AT 2,i-1;"-"
8120 LET c=f(i)
8130 IF c=0 THEN  GO TO 8170
8135 PRINT AT 2,i-1;"-"
8140 FOR j=1 TO nr
8150 LET p$(j,c)=c$(j,i)
8160 NEXT j
8170 NEXT i
8180 FOR i=1 TO nr
8190 PRINT AT 2+i,16;p$(i)
8200 NEXT i
8210 RETURN
8220 LET sy=nr+4
8230 FOR i=sy TO 20
8240 PRINT AT i,0;TAB 31;" "
8250 NEXT i
8260 RETURN
9999 REM fin
```

Anotaciones para el programa "Análisis de la transposición por columnas completas"

Líneas	
10	Comentario identificador del programa.
20-60	El programa avisa de que va a cargar de cinta las tablas de frecuencias, y se produce la carga.
70-100	Se limpia la pantalla, aparece el título y el programa pide la introducción del texto.
100-240	Se quitan los espacios del texto; si el texto leído es "0" el programa termina. Aparece un signo de error si la cadena no contiene caracteres. Las letras en mayúsculas se pasan a minúsculas.
250-380	El programa calcula el número de factorizaciones posibles de la longitud del texto.
390-420	Se imprime el texto junto con la factorización.
430-640	El programa permite al usuario seleccionar la factorización.
430-450	El programa imprime formas de factorizar la longitud del texto.
460-515	Hay un ciclo hasta que se pulse una tecla. El "0" hace terminar el programa; "c" vuelca el contenido de la pantalla en la impresora; espacio hace que el programa continúe, y cualquier otra tecla hace que el programa imprima el cálculo de las vocales por filas.
520-640	El programa imprime el cálculo de vocales por filas para cada forma de factorización.
650-670	El programa espera la introducción de un código para seleccionar una factorización determinada. Se puede introducir una "c" para copiar la pantalla en la impresora. Se comprueba el dato para ver si es un número aceptable, y si no es así hay que volver a introducirlo.
680-780	Se mete el texto en un bloque de una dimensión de prueba y se imprime en la pantalla.
790-830	Se pide al usuario que pruebe con una columna del bloque.
840-865	Hay que pulsar una tecla.
867	Si es "n", el bloque de prueba se borra y el usuario puede realizar una serie de pruebas.
870	Si es "b", se borran las dimensiones del bloque y el usuario puede empezar de nuevo con un bloque de tamaño diferente.
880	Si es "c", la pantalla se vuelca en la impresora.
890	Si es "0", el programa termina.

Líneas	
910-1153	Calcula las probabilidades relativas de contacto izquierdo y derecho para dos columnas adyacentes de prueba; "l" para izquierda, "r" para derecha.
1160-1240	Si es "d", borra una columna de prueba del bloque.
1250-1300	Si es "i", coloca una columna en blanco en el bloque (es decir, abre un hueco).
1301-1308	Si es "w", escribe una columna dentro del bloque.
1310-1319	Si es "p", imprime las probabilidades relativas de contacto derecho para un par de letras.
1320-1340	Suena la alarma en caso de error.
1350-1390	Si es "s", imprime el texto final.
8000-8040	Rutina para aceptar y comprobar un número de columna.
8050-8090	Rutina para aceptar la posición para una operación de columna.
8100-8210	Rutina para imprimir el bloque de prueba.
8220-8260	Borra un trozo de la pantalla.
9999	Punto de terminación del programa.

Instrucciones de uso del programa "Análisis de la transposición por columnas completas"

El programa de análisis es estructuralmente similar al programa de cifrado y descifrado. Carga las tablas de frecuencias como hace el programa de ayuda monoalfabética y lee el texto, quitando los caracteres no válidos.

El programa factoriza la longitud del mensaje y permite al usuario seleccionar la factorización. Una vez elegida, se prepara un bloque de prueba. Se pueden insertar columnas dentro del bloque y ver qué columnas son más probablemente adyacentes, por medio de pulsar las siguientes teclas:

"w"	Escribe una columna en el bloque.
"d"	Borra una columna del bloque.
"i"	Inserta una columna en blanco en el bloque.
"l", "r"	Imprime las probabilidades relativas de contacto izquierdo y derecho, respectivamente.
"p"	Imprime la probabilidad relativa de contacto de un par de letras.
"b"	Empieza de nuevo y pone unas nuevas dimensiones al bloque.

"n" Borra el bloque existente, pero continúa con las mismas dimensiones.
"c" Copia la pantalla en la impresora.
"s" Imprime el texto final.
"0" Terminación.

En cuanto uses un poco el programa le cogerás el truco. Recuerda que tienes que tener las tablas de frecuencias en una cinta. ¡Los criptogramas de práctica están donde siempre!

Resolución de transposiciones de itinerario

El principio para descifrar esta clave es de nuevo el de anagramas múltiples, mencionado anteriormente. Técnicamente es posible escribir programas que lleven a cabo este trabajo y, de hecho, se adapta bien a las capacidades de los modernos ordenadores, incluso con tipos de ruta muy complicados.

Los anagramas por ordenador no son difíciles de programar. Sin embargo, los programas resultantes tienden a ser demasiado lentos en los ordenadores personales (especialmente aquellos que usan BASIC interpretado). El autor intentó desarrollar un programa que pudiera hacer anagramas múltiples para redes rectangulares, pero pronto fue obvio que tardaría, en general, demasiado. Pero no todo está perdido, ya que el programa cifrador por transposición de itinerario que se dio en el capítulo 6 nos puede ser bastante útil. La razón es que en este programa las rutas a menudo tienen partes comunes, por ejemplo, una columna, fila o diagonal concreta.

Para analizar un criptograma, simplemente tienes que ir probando rutas hasta que aparezca algún fragmento del texto original. Teniendo en cuenta la ruta usada, será fácil recobrar los fragmentos del texto. A continuación tienes un ejemplo.

Ejemplo 7.1

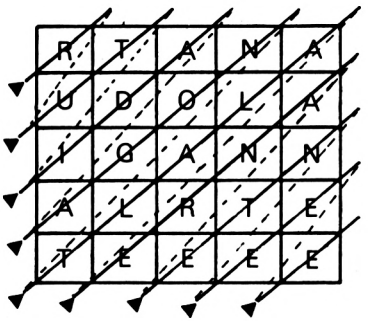
Criptograma:

RTANA UDOLA IGANN
ALRTE TEEEE

Primero escribimos el criptograma en una red como ésta:

R	T	A	N	A
U	D	O	L	A
I	G	A	N	N
A	L	R	T	E
T	E	E	E	E

Probemos ahora algunas rutas. Las rutas de filas y columnas no parecen muy prometedoras; luego probamos una diagonal, como:

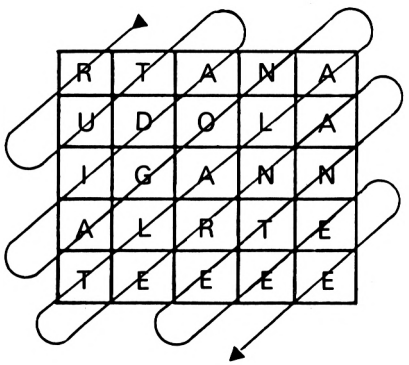


Según esto, el texto original sería:

RUTIDAAGONTLALAERNAETNEEE

y vemos que hay partes que parecen fragmentos de palabras.

Las primeras tres letras sugieren la palabra RUTA y el trozo que pone IDAAGON podría ser DIAGONAL. Un buen sistema para proceder ahora es reordenar este texto de forma que vayan saliendo palabras enteras. Por ejemplo, si cambiamos de orden las letras IDA del principio, nos quedaría RUTADIAGON, que ya parece tener bastante significado. Esto nos permite suponer que nuestra ruta tiene partes en común con la ruta verdadera. Teniendo estos factores en cuenta se recompone la ruta verdadera:



Y así vemos que la ruta original era una "RUTA DIAGONAL ALTERNANTE", que es, desde luego, el texto original.

Resolución de transposiciones con rejilla

La resolución de este tipo de transposiciones es más difícil que la resolución de las dos anteriores. Puedes aplicar los métodos de reordenación que se han usado antes, pero necesitarás un ordenador mucho más rápido del que tienes. Sin embargo, hay un método bueno de ataque a este problema, llamado método de la "palabra probable".

La base de este método es que tú sepas que haya una gran posibilidad de que una palabra concreta aparezca en el texto original. En el caso de rejillas giratorias este método es el más potente. Si tienes una palabra posible, puedes usarla para guiarte hacia la solución. En el ejemplo que sigue la palabra posible es INTERESANTES:

Ejemplo

EARSLE SPARSS ASONPA
NIOLNT ABTBEA BESLER

El primer paso es escribirlo en una red:

E	A	R	S	L	E
S	P	A	R	S	S
A	S	O	N	P	A
N	I	O	L	N	T
A	B	T	B	E	A
B	E	S	L	E	R

Ahora vamos a intentar colocar la palabra probable en la red. En este caso es fácil, ya que esta palabra tiene tres letras que no aparecen en el resto de la red: T, I y la N. Y además es razonable suponer que estas letras tienen que estar más o menos cercanas en la red. De momento, podemos asegurar que la N y la T que están juntas se escribieron también a la vez. Mientras que la otra T se tuvo que escribir en la siguiente postura de la rejilla.

E	A	R	S	L	E
S	P	A	R	S	S
A	S	O	N	P	A
N	I	O	L	Ⓝ	Ⓣ
A	B	🅃	B	E	A
B	E	S	L	E	R

Vamos a adoptar la convención de usar círculos, cuadrados, triángulos y diamantes, respectivamente, para denotar posiciones sucesivas de la red, en ese orden. Siguiendo este proceso podemos determinar inmediatamente más posiciones de la red. Se hace rotando la rejilla imaginaria y convirtiendo los círculos en cuadrados, los cuadrados en triángulos, y así sucesivamente. De esta forma añadimos más información a nuestra red:

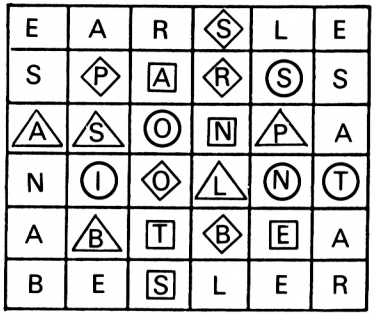
E	A	R	S	L	E
S	P	A	R	S	S
A	S	O	N	P	A
N	I	O	L	N	T
A	B	T	B	E	A
B	E	S	L	E	R

Podemos seguir avanzando. Es evidente que la I se escribió a la vez que NT, para formar INTERESANTE, luego también le corresponde un círculo. También se puede suponer que la N que todavía no está marcada viene antes de la T recuadrada, luego también llevará un cuadrado. Marcamos, pues, estas dos letras y hacemos rotar de nuevo nuestra red imaginaria:

E	A	R	S	L	E
S	P	A	R	S	S
A	S	O	N	P	A
N	I	O	L	N	T
A	B	T	B	E	A
B	E	S	L	E	R

Ahora vemos que entre la T y la S con cuadrados debe haber una E. Hay dos posibilidades, pero la E más inferior queda descartada, pues si fuera del tipo cuadrado, la A de la sexta columna y la quinta fila debería ser un círculo, lo que es imposible al venir antes una T. Por

tanto, marcamos con un círculo la E que nos ha quedado y hacemos rotar de nuevo la red:



E	A	R	S	L	E
S	P	A	R	S	S
A	S	O	N	P	A
N	I	O	L	N	T
A	B	T	B	E	A
B	E	S	L	E	R

Continuando con este proceso, al final se llega a la frase: LAS PALABRAS PROBABLES SON INTERESANTES, con una E al final para rellenar la red.

El método de la palabra probable no es muy complicado de hacer a mano. Usado conjuntamente con el sistema de probabilidad de contacto resuelve fácilmente los criptogramas de este tipo. Tienes que empezar suponiendo la palabra probable, pero luego el proceso es rápido. Aquí tienes el programa:

```
  10 REM ANALISIS POR LA REJILLA
                DE CARDANO
  20 PRINT AT 11,4;"PONGA LA CIN
TA CON DATOS";AT 12,3;"PULSE LUE
GO CUALQUIER TECLA"
  30 BEEP 1,12
  40 IF INKEY$="" THEN  GO TO 40
  50 LOAD "" DATA e()
  60 LOAD "" DATA t()
  70 CLS
  80 PRINT "PROGRAMA DE ANALISIS
 'REJILLA DE CARDANO'"
  90 PRINT AT 2,2;"TEXTO"
 100 INPUT t$
 110 IF t$="0" THEN  GO TO 9999
 120 FOR i=1 TO LEN t$
 130 IF i>LEN t$ THEN  GO TO 200
 140 IF t$(i)>="a" AND t$(i)<="z
" THEN  GO TO 200
```

```
 150 LET r$=""
 160 IF i>1 THEN  LET r$=t$( TO
i-1)
 170 IF i<LEN t$ THEN  LET r$=r$
+t$(i+1 TO )
 180 LET t$=r$
 190 GO TO 130
 200 NEXT i
 210 LET lt=LEN t$
 220 IF lt=0 THEN  GO TO 240
 230 IF lt/36=INT (lt/36) THEN
GO TO 260
 235 LET t$=t$+"z"
 240 LET lt=lt+1
 250 GO TO 230
 260 PRINT AT 2,0;"TEXTO : ";t$
 270 LET nb=INT (lt/36)
 310 LET ca=CODE "a"-1
 370 PRINT AT 21,0;"PULSE CUALQU
IER TECLA (C=COPY)."
 380 LET r$=INKEY$
 390 IF r$="" THEN  GO TO 380
 395 IF r$="0" THEN  GO TO 9999
 400 IF r$<>"c" THEN  GO TO 430
 410 COPY
 420 GO TO 380
 430 CLS
 440 DIM g(6,6)
 450 DIM a(6,6)
 460 PLOT 100,164
 470 DRAW 56,0
 480 DRAW 0,-56
 490 DRAW -56,0
 500 DRAW 0,56
 510 PRINT AT 0,13;"123456"
 520 FOR i=1 TO 6
 530 PRINT AT i+1,11;i
 540 NEXT i
 541 LET nh=0
 545 LET r$=""
 550 GO TO 700
 560 PRINT AT 21,0;"PULSE c,d,h,
l,r,p,t,n o 0"
 570 LET r$=INKEY$
```

```
580 IF r$="" THEN  GO TO 570
590 PRINT AT 21,0;TAB 31
600 IF r$<>"c" THEN  GO TO 630
610 COPY
620 GO TO 560
630 IF r$<>"d" THEN  GO TO 690
640 GO SUB 8000
650 LET g(y,x)=0
660 PRINT AT 1+y,12+x;" "
670 LET nh=nh-1
680 GO TO 560
690 IF r$<>"h" THEN  GO TO 740
700 GO SUB 8000
710 LET g(y,x)=1
720 PRINT AT 1+y,12+x;" "
725 LET nh=nh+1
730 GO TO 560
740 IF r$<>"l" AND r$<>"r" THEN
 GO TO 1105
745 GO SUB 8200
750 GO SUB 8000
753 LET xx=x
757 LET yy=y
760 IF r$="l" THEN  GO TO 830
770 LET x=x+1
780 IF x<=6 THEN  GO TO 915
790 LET x=1
800 LET y=y+1
810 IF y>6 THEN  GO TO 560
820 GO TO 880
830 LET x=x-1
840 IF x>=1 THEN  GO TO 915
850 LET x=6
860 LET y=y-1
870 IF y<1 THEN  GO TO 560
915 LET p=0
917 FOR i=1 TO nb
920 FOR j=1 TO 2
960 IF r$="r" THEN  LET p=p+t(C
ODE t$((i-1)*36+(yy-1)*6+xx)-ca,
CODE t$((i-1)*36+(y-1)*6+x)-ca)
970 LET x=7-x
980 LET y=7-y
990 LET xx=7-xx
```

```
1000 LET yy=7-yy
1010 LET r$=CHR$ (CODE "r"+CODE
"l"-CODE r$)
1020 NEXT j
1025 NEXT i
1030 LET in=1
1040 FOR i=1 TO 4
1050 GO SUB 8100
1060 IF g(x,y)=1 THEN  LET in=0
1070 NEXT i
1080 PRINT  INVERSE in;x;",";y;
INVERSE 0;": ";p,
1090 IF PEEK 23689>5 OR PEEK 236
88=17 THEN  GO TO 760
1100 GO TO 560
1105 IF r$="n" THEN  GO TO 430
1110 IF r$<>"p" THEN  GO TO 1200
1120 GO SUB 8200
1130 INPUT "Letras?";l$
1140 IF LEN l$<>2 THEN  GO TO 11
30
1150 LET l1=CODE l$(1)-ca
1160 LET l2=CODE l$(2)-ca
1170 IF l1<1 OR l1>26 OR l2<1 OR
 l2>26 THEN  GO TO 1130
1180 PRINT  INVERSE 1;l$; INVERS
E 0;": ";t(l1,l2)
1190 GO TO 560
1200 IF r$<>"t" THEN  GO TO 1460
1205 IF nh=9 THEN  GO TO 1210
1207 BEEP 1,0
1208 GO TO 560
1210 LET rf=1
1211 FOR y=1 TO 6
1212 FOR x=1 TO 6
1213 LET a(y,x)=g(y,x)
1214 NEXT x
1215 NEXT y
1219 FOR i=1 TO 4
1220 GO SUB 8200
1225 FOR j=1 TO nb
1230 FOR k=1 TO 4
1240 FOR y=1 TO 6
1250 FOR x=1 TO 6
```

```
1260 IF a(y,x)<>rf THEN  GO TO 1
270
1261 PRINT t$((j-1)*36+(y-1)*6+x
);
1262 LET a(y,x)=0
1263 LET a(x,7-y)=3-rf
1270 NEXT x
1280 NEXT y
1290 LET rf=3-rf
1300 NEXT k
1310 NEXT j
1320 PRINT AT 21,0;"PULSE c,n,r,
s o 0."
1330 LET r$=INKEY$
1340 IF r$="" THEN  GO TO 1330
1345 PRINT AT 21,0;TAB 31
1350 IF r$<>"c" THEN  GO TO 1380
1360 COPY
1370 GO TO 1320
1380 IF r$<>"n" THEN  GO TO 1410
1381 FOR y=1 TO 6
1382 FOR x=1 TO 6
1383 IF a(y,x)<>rf THEN  GO TO 1
386
1384 LET a(y,x)=0
1385 LET a(x,7-y)=3-rf
1386 NEXT x
1387 NEXT y
1388 LET rf=3-rf
1390 NEXT i
1400 GO TO 1219
1410 IF r$="r" THEN  GO TO 560
1420 IF r$="s" OR r$="0" THEN  G
O TO 9999
1430 PRINT AT 21,0;"?"
1440 BEEP 1,0
1450 GO TO 1320
1460 IF r$="0" THEN  GO TO 9999
1470 PRINT AT 21,0;"?"
1480 BEEP 1,0
1490 GO TO 560
8000 INPUT "Posicion:x,y?";x;" "
;y
8005 IF x=0 OR y=0 THEN  GO TO 9
```

```
999
8010 IF x<1 OR x>6 OR x>INT x OR
 y<1 OR y>6 OR y>INT y THEN  GO
TO 8000
8020 IF r$="d" OR r$="l" OR r$="
r" THEN  GO TO 8080
8030 FOR i=1 TO 4
8040 GO SUB 8100
8050 IF g(y,x)<>0 THEN  GO TO 80
90
8060 NEXT i
8070 RETURN
8080 IF g(y,x)=1 THEN  GO TO 807
0
8090 BEEP 1,0
8095 GO TO 8000
8100 LET s=y
8110 LET y=7-x
8120 LET x=s
8130 RETURN
8200 FOR i=10 TO 20
8210 PRINT AT i,0;TAB 31;" "
8220 NEXT i
8230 PRINT AT 10,0;
8240 RETURN
9999 REM fin
```

Anotaciones para el programa "Análisis por la rejilla de Cardano"

Líneas	
10-60	Carga las tablas de frecuencia, de la misma forma que se hizo en otros programas de análisis.
70-260	Lee y comprueba el texto.
370-420	Acepta una tecla del usuario para continuar.
430-540	Prepara la pantalla.
560-590	Imprime el menú de opciones de que se dispone.
600-620	"c": copia la pantalla en la impresora.
630-680	"d": borra un agujero de la rejilla.
690-730	"h": hace un agujero en la rejilla.

Líneas	
740-1100	"l" y "r": imprime los mejores contactos izquierda y derecha, usando las probabilidades relativas de contacto.
1105	"n": empieza de nuevo con una rejilla nueva.
1110-1400	"p": imprime la probabilidad de contacto derecho para un par de letras.
1200-1450	"t": imprime el texto en los agujeros actuales.
1200-1310	Se imprime el texto.
1320-1340	Menú secundario.
1350-1370	"c": copia la pantalla en la impresora.
1470-1490	Rutina de alarma del menú principal.
8000-8095	Subrutina de lectura de las coordenadas x,y.
8200-8240	Subrutina para borrar la información antigua.
1380-1400	"n": imprime el siguiente bloque.
1410	"r": vuelve al menú principal.
1420	"s" o "0": terminación.
1430-1450	Alarma de error.
1460	En el menú principal "0" hace terminar al programa.

Instrucciones del programa "Análisis por la rejilla de Cardano"

Ya le habrás cogido el truco a este tipo de programas. Es un proceso controlado por un menú donde tú creas los agujeros basándote en la palabra probable, y luego continúas haciendo más agujeros por medio de las tablas de contactos. Las opciones del menú principal son las siguientes:

"c":	Copia la pantalla en la impresora.
"d":	Borra un agujero.
"h":	Crea un agujero.
"l", "r":	Muestra las probabilidades de contacto izquierdo y derecho.
"p":	Muestra las probabilidades relativa de contacto de un par de letras.
"t":	Imprime el texto.
"n":	Empieza de nuevo con una rejilla en blanco.
"0":	Fin.

El programa va explicando cada paso a medida que funciona.
Ya sabes dónde encontrar unos cuantos ejercicios.

Criptogramas de práctica

Columnas

1. fnseoeaoeosntaodaemracuelrseeeeup
dUdsoaeipsodnoeoctdzooudetlrseae
zclsrpeoseucssadensxrsssgmunmoid
iolidsleiatgorlplseafcratrescils
aa

2. mqocebrnbruodietnhnpiiurezyanzda
nomesricsculemnpsavzarnuihucoceu
caoiaerieaedeznuusaalaercfsieliq
oooeeisrojieldatleauuonamumlrlnc
eaheedaerohadtihdvaebetlsids

3. paaeinlcuacrounsdamranuuhohnmnna
pelmdscassilsinoezstuornеatraamr
aourоatecqrtaaoeelxiooisataiseec
edmooecdcevssbauoiripednomelesim
criоendcsolnemovsnlootlosnsboaom
ntcsedyinitltaiirUapddyonaoieosi
mnoeatmn

4. lneemsnnsadtrnitnraidcienzeeidoe
oiapanetmohecccoadedzednubtdaucde
z

5. lncieroatusaiehivoegoadosnmpeaed
sgnobidrrsbantsaavrlecaerlceiazo
dseelriqomanlreisntz

Itinerario

6. damsmicoeavehecadarnladbuaiotdhs
mnooasitniilnicmeeaeoudcobennnnsd
euieosemlznnzzzzzzzzzzozzzzrzzzze
zzzz

7. crslelaipesebtioorausncolatesidr
retaaaaanussttejmlotocerаecosssso
mepdaricrenbeebaelnslaeahyoslrao
mcldoiaadzsrsmzzatvzzzzsuzzzzzz

8. orgolocsetsoledtnocaimicesotneir
aidsonsotlucoevalaedadrsedaricer
galedaisapszsenozzzzzzzzzzzzzzzzz
zzzz

9. l t t d e a s u s e e r e u e a z p t r e l n g a c a l l d i a
a i a s u s t a c o o p a l i s s n a a s i n l i r a r h o r o
d t t f a s a s m o e n e e s l h o n o e r e b o e s m s g i i
o n n o s z z z z z z z z z z z z z z z z z z z z z z z z z

10. a t b e e m i e d l p n p o a o r e n m c i d r o e u e d o r f
t a e z a e h x a l n r i d r e i g a l e r e c o n a e e m s r
n r s i t c t i m n o z z z z e z z z z z z z z z a z z z z z z
z z z z

Cardano

11. Palabra probable: méritos

r i t y c o o s s n s e i n o g u i o p o a s c r m i e n d s m
e e r n t a z p o r z z z q u e z z z m i a t a q m o t u e d u
v o e g o u n a

12. Palabra probable: brutos

s l s o a b r s u h o m v e o t c o o s m e t a s s s b q r e n
u e e l a l r e t e s g t a s i a l q e e n a u p n i e t o d e
r n s n a n n o u s j e z z z r z a e r z z e z z z n s l z z z
z z z z a z s m z z z z z z

13. Palabra probable: cuerpo

o m i m u e n r m e n a p o a t o s u e c p u e n e r q d j e c
m i c a e u e s i s a p h e h o i e r a m b n h i a s t a g a s
a e n t d e m c

14. Palabra probable: elegante

n l l o e a e r s n s v a q p i a u i m l e r t b o e o i p e c
r p e i e l a r r e e y a e e l p u a n e n r l g a a m a a c s
u e j a n t g l t a u i i o s r u e r n p c a l e a r a n s a a
h v a e n n o s a l c t l o e r a z l z a z r z z s z a z c z r
z o z n s z e z e z l a z z z s

15. Palabra probable: vestido

l a r e t n y b a n o e i d o a e n d a s s t e s a o i t e v m
u a b r s v a z z r i o a e z l n z z s z z t i z a o d z c z z
o p z a s z z z

8
Cifrados más complejos

Los cifrados de este capítulo son todos variaciones de los cifrados por sustitución. Los tres tipos que vamos a ver son los poligráficos, los polialfabéticos y los fraccionarios. Un cifrado poligráfico es aquel en el cual en lugar de sustituir una letra por otra se cogen grupos de dos o más. Un cifrado polialfabético es aquel en el que se sustituyen letras individuales, pero se utilizan más de un alfabeto cifrado. Y un cifrado fraccionado es aquel en el que se pueden considerar letras individuales representadas por una o más letras u otros símbolos, y donde se trabaja con estos símbolos más que con las letras mismas.

Estas claves son mucho más sofisticadas que las que se han tratado hasta ahora en el libro. Sin embargo, pueden resolver, y se han elegido algunos ejemplos para ilustrar las clases de métodos que se usan en el criptoanálisis. En concreto, los tres cifrados de este capítulo son el cifrado Hill, el citado Gronsfeld y el cifrado Bífido. Vamos a estudiarlos por este orden.

El método Hill: un cifrado poligráfico

El nombre es debido a un americano que lo publicó por primera vez en el año 1930. Para utilizarlo, se escribe el alfabeto en orden normal y, a continuación, se escribe debajo de cada letra el número de su posi-

ción en el alfabeto. El truco consiste en tener una matriz de cuatro posiciones. (Ya habrás estudiado en las matemáticas del colegio las matrices, pero si no es así, no te preocupes, ya que son fáciles de entender e iremos paso a paso.) El cifrado se lleva a cabo cogiendo las letras del texto original de dos en dos, escribiendo sus dos números y multiplicándolos por la matriz que se indica más adelante. Estudia el siguiente ejemplo y lo entenderás.

Ejemplo del método Hill

Primero escribe el alfabeto y los números:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	Ñ	O	P	Q	R	S	T	U	V	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Supongamos que tenemos la matriz

$$\begin{pmatrix} 4 & 5 \\ 3 & 4 \end{pmatrix}$$

como clave.

El mensaje es

LLEGUE VI VENCI

Primero escribimos los números que corresponden a estas letras:

12 12 5 7 22 5 23 9 23 5 14 3 9

Si el número de letras del texto original resulta impar, se añade una letra adicional al final, como se ha hecho en este caso. A continuación, se hace una multiplicación un poco especial: Para cada par de números n1, n2 hallamos N1, N2, según la fórmula:

$$N1 = (m_{11} \times n_1 + m_{12} \times n_2) \bmod 26$$

$$N2 = (m_{21} \times n_1 + m_{22} \times n_2) \bmod 26$$

donde

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$$

es la matriz clave, y "(A) mod 26" es el resto de dividir A entre 26.

El resultado de hacer esto en nuestro ejemplo es:

4, 6, 3, 17, 9, 8, 7, 1, 13, 11, 19, 2, 10, 1: texto numérico.

El siguiente paso es simplemente sustituir los números por las letras correspondientes, según la tabla que escribimos al principio:

D F C P I H G A M K R B J A: texto alfabético.

El proceso para descifrar es exactamente el mismo, con la diferencia de que se usa la inversa de la matriz clave. La inversa de la matriz:

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$$

es la matriz

$$\begin{pmatrix} m_{22}/d & -m_{12}/d \\ -m_{21}/d & m_{11}/d \end{pmatrix}$$

donde d es el valor

$$m_{11} \times m_{22} - m_{12} \times m_{21}$$

(d representa el determinante de la matriz. Sólo las matrices cuyo determinante es distinto de cero tienen inversa, luego si no usas matrices de este tipo no podrás descifrar el mensaje. Ten cuidado).

En nuestro ejemplo la matriz clave tenía por determinante 1, luego su inversa es:

$$\begin{pmatrix} 4 & -5 \\ -3 & 4 \end{pmatrix}$$

Si ahora realizas los pasos anteriores, pero con esta matriz, aparecerá el texto original.

Es excepcionalmente fácil escribir el programa para cifrar y descifrar por el método Hill, ya que todos los pasos son esencialmente aritméticos. Aquí está el programa:

```
  10 REM HILL
  15 DATA 1,9,21,15,3,19,0,7,23,
11,5,17,25
  20 PRINT "PROGRAMA DE CIFRADO
HILL"
  30 PRINT AT 2,2;"MODO"
  40 INPUT m$
  50 IF m$="0" THEN  GO TO 9999
  60 IF m$="c" OR m$="d" THEN  G
O TO 90
  70 PRINT AT 2,0;"?"
  80 GO TO 40
  90 PRINT AT 2,0;"MODO : ";m$
 100 PRINT AT 4,2;"MATRIZ"
 110 INPUT a;" ";b;" ";c;" ";d
 120 PRINT AT 6,0;TAB 31
 130 LET l=a*d-b*c
 133 GO SUB 1000
 137 LET det=l
 140 IF l<>0 THEN  GO TO 180
 150 PRINT AT 6,0;"NO EXISTE MAT
RIZ INVERSA"
 160 PRINT AT 4,0;"?"
 170 GO TO 110
 180 IF l/2>INT (l/2) AND l/13>I
NT (l/13) THEN  GO TO 210
 190 PRINT AT 6,0;"EL DETERMINAN
TE NO ES ADECUADO"
 200 GO TO 160
 210 PRINT AT 4,0;"MATRIZ : ";a;
",";b;",";c;",";d
 220 PRINT AT 6,2;"TEXTO"
 230 INPUT t$
 240 IF t$="0" THEN  GO TO 9999
 260 FOR i=1 TO LEN t$
 270 IF i>LEN t$ THEN  GO TO 330
 280 IF t$(i)>="a" AND t$(i)<="z
" THEN  GO TO 330
 290 LET r$=""
 300 IF i>1 THEN  LET r$=t$( TO
i-1)
 310 IF i<LEN t$ THEN  LET r$=r$
+t$(i+1 TO )
 320 LET t$=r$
```

```
325 GO TO 270
330 NEXT i
340 LET lt=LEN t$
350 IF lt>1 THEN  GO TO 380
360 PRINT AT 6,0;"?"
370 GO TO 230
380 IF lt/2=INT (lt/2) THEN  GO
TO 410
390 LET t$=t$+"z"
400 LET lt=lt+1
410 PRINT AT 6,0;"TEXTO : ";t$
415 LET ca=CODE "a"-1
420 IF m$="c" THEN  GO TO 500
425 FOR i=1 TO 25 STEP 2
426 READ j
427 IF i=det THEN  LET r=j
428 NEXT i
430 LET i=a
433 LET a=d
437 LET d=i
440 LET b=-b
445 LET c=-c
450 LET l=a*r
453 GO SUB 1000
457 LET a=l
460 LET l=b*r
463 GO SUB 1000
464 LET b=l
465 LET l=c*r
466 GO SUB 1000
467 LET c=l
470 LET l=d*r
473 GO SUB 1000
477 LET d=l
480 PRINT
490 PRINT "MATRIZ INVERSA : ";a
;",";b;",";c;",";d
500 PRINT
510 FOR i=1 TO lt STEP 2
520 LET l1=CODE t$(i)-ca
530 LET l2=CODE t$(i+1)-ca
540 LET l=a*l1+b*l2
550 GO SUB 1000
560 PRINT CHR$ (l1+ca);
```

```
 570 LET l=c*11+d*12
 580 GO SUB 1000
 590 PRINT CHR$ (11+ca);
 600 NEXT i
 610 GO TO 9999
1000 IF l>=0 AND l<26 THEN  GO T
O 1040
1010 IF l<0 THEN  LET l=l+26
1020 IF l>=26 THEN  LET l=l-26
1030 GO TO 1000
1040 LET 11=l
1050 IF l=0 THEN  LET 11=26
1060 RETURN
9999 REM fin
```

Programa de cifrado "Hill". Anotaciones

Líneas	
10	Comentario identificador del programa.
15	Datos en aritmética en módulo 26.
20	Impresión del título del programa.
30-90	Se pide el modo; si es "0" se termina. Si no es ni "c" ni "d" hay que volver a introducirlo. Cuando el modo es aceptado se imprime en la pantalla.
100-210	Se pide la introducción de la matriz. Si el determinante es igual a cero, se avisa del error y hay que volver a introducir la matriz. Cuando la matriz es correcta se imprime.
220-370	Se pide la introducción del texto. Si es "0" se termina. Se quitan los espacios y los caracteres no alfabéticos y se comprueba que el texto resultante tenga más de una letra.
380-400	Si es necesario se rellena el texto para conseguir un número par de letras.
410-420	Imprime la cabecera, inicializa el proceso y selecciona entre cifrado y descifrado, según el modo.
425-428	Selecciona el inverso del determinante de la matriz.
430-445	Forma el transpuesto de la matriz.
450-477	Forma la matriz inversa.
480-500	Imprime la matriz inversa.
510-600	Se usa la matriz si se está cifrando, y la matriz inversa si se está descifrando.

Líneas	
610	Salta al fin del programa.
1000-1060	Ajusta los valores en módulo 26.
9999	Línea de fin de programa.

Instrucciones de uso para el programa de cifrado "Hill"

Como es usual se pide el modo. Puede ser "c" o "d", con sus significados habituales.

Para el cifrado Hill la clave es una matriz 2 × 2. El programa pide la introducción de cada uno de los elementos de la matriz. Comprueba que el determinante es adecuado y vuelve a leer la matriz si no lo es. Una vez la matriz es correcta, se lee el texto. Los espacios y los caracteres no alfabéticos se quitan y se produce un error si el texto resultante no tiene caracteres alfabéticos. En este último caso hay que volver a introducir el texto.

Una vez se dispone de un texto adecuado, el programa lo rellena hasta conseguir un número par de letras y procede a cifrar o a descifrar, según indique el modo. En ambos casos se imprime el texto leído, seguido del texto cifrado —o descifrado, según corresponda.

Se sale introduciendo "0" o bien por terminación normal del programa.

Si coges algunos de los criptogramas de prácticas y los introduces en los programas de análisis de frecuencias que se usan en la sustitución monoalfabética, verás, especialmente con mensajes extensos, que los contadores de frecuencia no coinciden con los que salen con la sustitución monoalfabética. Esto hace que el cifrado Hill sea mucho más difícil de descifrar. Básicamente, puedes hacerlo por medio de disponer de suficiente texto para que las frecuencias de los digramas empiecen a mostrar una estructura determinada; se necesita, al menos, 26 veces el texto necesario para descifrar uno monoalfabético. Hay métodos más sofisticados, pero no vamos a tratar de ellos en este libro.

El método Gronsfeld: un cifrado polialfabético

El cifrado Gronsfeld es del tipo conocido como polialfabéticos. Esto significa que se usan más de un alfabeto cifrado para poner en clave el mensaje y cambian entre sí a medida que pasas de una letra del texto original a otra. Para hacer esto debes tener un conjunto de alfabetos cifrados y una serie de claves que te dicen qué alfabeto se debe usar para poner en clave cada letra.

Antes de la era de los ordenadores se solía utilizar una tabla para tener los alfabetos y para indicar cuál correspondía a cada dígito o letra de la clave. Aquí tienes una tabla para el método Gronsfeld:

```
   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 : C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
1 : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
2 : F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
3 : H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
4 : L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
5 : N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
6 : R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
7 : T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
8 : X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
9 : C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
```

Ahora cogemos una serie de dígitos como clave. En este caso usaremos 0271983654 (no es el teléfono de nadie, así que no te molestes en llamar).

Usaremos la tabla y la clave para cifrar el mensaje

FELIPE ESTABA ENFERMO FELIPE MURIO

Para cifrar debemos escribir la clave debajo del texto original el número de veces que sea necesario:

```
FELIPE  ESTABA  ENFERMO  FELIPE  MURIO
027198  365402  7198365  402719  83654
```

Ahora ciframos el mensaje simplemente por sustitución, pero para cada letra se coge el alfabeto correspondiente al número de la clave que tiene debajo, según indica la tabla.

FGSJYM HYYEBC LOOMUST JENPQN UXXNS

Si te fijas en este ejemplo y en los criptogramas de prácticas, verás que las frecuencias de las letras del texto cifrado no coinciden con las de los monoalfabéticos.

Este programa hará por ti el cifrado y descifrado de Gronsfeld. En parte es parecido al programa de la clave del César del capítulo 2.

```
  10 REM GRONSFELD
  20 PRINT "PROGRAMA DE CIFRAR G
RONSFELD"
  30 PRINT AT 2,2;"MODO Y NUMERO
 CLAVE"
  40 INPUT m$
  50 IF m$="0" THEN  GO TO 9999
  60 LET lm=LEN m$
  70 IF lm<2 THEN  GO TO 90
  80 IF m$(1)="c" OR m$(1)="d" T
HEN  GO TO 110
  90 PRINT AT 2,0;"?"
 100 GO TO 40
 110 DIM k(lm-1)
 120 FOR i=2 TO lm
 130 LET k$=m$(i)
 140 IF k$<"0" OR k$>"9" THEN  G
O TO 90
 150 LET k(i-1)=VAL k$
 160 NEXT i
 170 PRINT AT 2,0;"MODO : ";m$(1
);" NUMERO CLAVE : ";m$(2 TO )
 180 PRINT AT 4,2;"TEXTO"
 190 INPUT t$
 200 IF t$="0" THEN  GO TO 9999
 210 LET lt=LEN t$
 220 IF lt>0 THEN  GO TO 250
 230 PRINT AT 4,0;"?"
 240 GO TO 190
 250 PRINT AT 4,0;"TEXTO : ";t$
 260 PRINT
 263 LET cs=CODE " "
 265 LET ca=CODE "a"
 267 LET cz=CODE "z"
 270 IF m$(1)="d" THEN  GO TO 37
0
 280 LET k=0
 290 FOR i=1 TO lt
 293 IF t$(i)<>" " THEN  GO TO 3
00
 295 LET l=cs
 297 GO TO 340
 300 LET k=k+1
 310 IF k=lm THEN  LET k=1
```

```
 320 LET l=CODE t$(i)+k(k)
 330 IF l>cz THEN  LET l=l-26
 340 PRINT CHR$ l;
 350 NEXT i
 360 GO TO 9999
 370 LET k=0
 380 FOR i=1 TO lt
 383 IF t$(i)<>" " THEN  GO TO 3
90
 385 LET l=cs
 387 GO TO 430
 390 LET k=k+1
 400 IF k=lm THEN  LET k=1
 410 LET l=CODE t$(i)-k(k)
 420 IF l<ca THEN  LET l=l+26
 430 PRINT CHR$ l;
 440 NEXT i
9999 REM fin
```

Observa que, para simplificar el programa, se usan diez alfabetos, cada uno diferenciado del anterior en una posición. Esta es la forma más usual de usar el cifrado Gronsfeld. La variación que hemos descrito en el texto no es, sin embargo, muy extravagante.

Anotaciones para el programa de cifrado "Gronsfeld"

Líneas	
10-20	Comentario identificador del programa e impresión del título.
30-160	Pide la introducción del modo y la clave; si es "0" el programa termina. Se comprueba la entrada —el modo debe ser "c" o "d" y la clave un número—. Como siempre, si hay algún error hay que volver a introducir los datos.
170-240	Imprime el modo y la clave, y pide la introducción del texto; termina si se introduce "0". Comprueba que el texto no esté vacío.
250-260	Imprime el texto y se prepara para cifrar o descifrar.
270	Selecciona entre cifrar o descifrar según el modo.
280-350	Imprime el texto cifrado.
360	Salta al final del programa.
370-440	Imprime el texto descifrado.
9999	Línea de fin de programa.

Instrucciones de uso del programa de cifrado "Gronsfeld"

Siguiendo la estructura normal, se pide la introducción del modo y la clave. Hay que introducirlo de la forma: "c" número o "d" número, donde "c" y "d" significan cifrar y descifrar, y el número es una secuencia de dígitos que se va a usar como clave. El programa comprueba que los datos sean correctos.

A continuación se lee el texto. Se imprime el texto leído, seguido del texto cifrado (si se está cifrando) o del texto original (si se está descifrando).

La introducción de "0" produce el mismo efecto que en el resto de los programas.

Si usas una clave larga, puede ser muy difícil romper los criptogramas Gronsfeld. Afortunadamente (para los criptoanalistas) las claves largas tienen algunos inconvenientes y es posible usar un método relativamente simple para descubrir la longitud de la clave. Una vez se conoce ésta, se hacen los contadores de frecuencia para aquellas posiciones del criptograma que fueron cifradas con el mismo dígito de la clave. Con una cantidad de texto suficiente, estos contadores empezarán a mostrar las características monoalfabéticas y el texto se podrá descifrar.

El método Bífido: un cifrado fraccionario

Para usar este método se escribe el alfabeto desordenado en un cuadrado de 5 × 5, en el cual las columnas y las filas están numeradas. Nuestro alfabeto está desordenado según la palabra clave SALUDO. Observa que al ser la red de 5 × 5 es obligatorio poner siempre juntas la I y la J y, por tanto, se cifran igual.

	1	2	3	4	5
1	S	A	L	U	D
2	O	B	C	E	F
3	G	H	IJ	K	M
4	N	Ñ	P	Q	R
5	T	V	X	Y	Z

Para cifrar el texto original se escribe éste, pero reemplazando cada letra por las dos coordenadas que le direccionan en el cuadrado. Por ejemplo, la G sería 31 y la Ñ 42.

Si el texto original es:

EN UN LUGAR DE LA MANCHA

el equivalente numérico es:

2 4 1 4 1 1 3 1 4 1 2 1 1 3 1 4 2 3 1

4 1 4 1 3 4 1 2 5 5 4 3 2 5 2 1 3 2 2

Ahora transponemos los dígitos leyendo por filas, pero escribiéndolos en columnas, como se indica a continuación:

2 1 1 3 4 2 1 1 2 1 1 1 4 2 5 3 5 1 2
↓↗↓↗...etc.
4 4 1 1 1 1 3 4 3 4 4 3 1 5 4 2 2 3 2

Por último, se pasan de nuevo a letras estos dígitos, sustituyendo cada par por la letra que les corresponde en la tabla inicial. Para nuestro mensaje nos queda:

EUSGN OLUCU ULNFY HVLB

Las frecuencias de estos criptogramas son distintas de las monoalfabéticas.

Aquí está el programa que hace el cifrado y descifrado Bífido.

```
  10 REM BIFIDO
  20 PRINT "PROGRAMA DE CIFRADO
'BIFIDO'"
  30 PRINT AT 2,2;"MODO Y PALABR
A CLAVE"
  40 INPUT m$
  50 IF m$="0" THEN  GO TO 9999
  60 IF LEN m$<2 THEN  GO TO 80
  70 IF m$(1)="c" OR m$(1)="d" T
HEN  GO TO 100
  80 PRINT AT 2,0;"?"
  90 GO TO 40
 100 DIM a(25)
 110 DIM l(25)
 115 LET ca=CODE "a"-1
 120 LET a=0
 130 FOR i=2 TO LEN m$
```

```
 140 LET c=CODE m$(i)-ca
 150 IF l(c)>0 THEN  GO TO 190
 160 LET a=a+1
 170 LET a(a)=c
 180 LET l(c)=a
 190 NEXT i
 200 FOR i=1 TO 25
 210 IF l(i)>0 THEN  GO TO 250
 220 LET a=a+1
 230 LET a(a)=i
 240 LET l(i)=a
 250 NEXT i
 260 PRINT AT 2,0;"MODO : ";m$(l
);TAB 31
 270 PRINT AT 4,0;"ALFABETO ALTE
RADO :"
 280 FOR i=0 TO 4
 290 FOR j=1 TO 5
 300 PRINT AT 4+i,20+j;CHR$ (a(i
*5+j)+ca)
 310 NEXT j
 320 NEXT i
 330 PRINT AT 10,2;"LONGITUD DEL
 BLOQUE"
 340 INPUT b
 345 IF b=0 THEN  GO TO 9999
 350 IF b>1 AND b=INT b THEN  GO
 TO 380
 360 PRINT AT 10,0;"?"
 370 GO TO 340
 380 PRINT AT 10,0;"LONGITUD DEL
 BLOQUE : ";b
 385 DIM b(2*b)
 390 PRINT AT 12,2;"TEXTO"
 400 INPUT t$
 405 IF t$="0" THEN  GO TO 9999
 410 FOR i=1 TO LEN t$
 420 IF i>LEN t$ THEN  GO TO 490
 430 IF t$(i)>="a" AND t$(i)<="y
" THEN  GO TO 490
 440 LET r$=""
 450 IF i>1 THEN  LET r$=t$( TO
i-1)
 460 IF i<LEN t$ THEN  LET r$=r$
```

```
+t$(i+1 TO )
 470 LET t$=r$
 480 GO TO 420
 490 NEXT i
 500 LET lt=LEN t$
 510 IF lt>1 THEN  GO TO 540
 520 PRINT AT 12,0;"?"
 530 GO TO 400
 540 PRINT AT 12,0;"TEXTO : ";t$
 550 PRINT
 560 IF m$(1)="d" THEN  GO TO 72
0
 570 FOR i=1 TO lt STEP b
 580 LET t=b-1
 590 IF i+t>lt THEN  LET t=lt-i
 600 FOR j=0 TO t
 610 LET l=CODE t$(i+j)-ca
 620 LET a=l(1)
 630 LET b(j+1)=INT ((a-1)/5)+1
 640 LET b(j+t+2)=a-5*(b(j+1)-1)
 650 NEXT j
 660 FOR j=0 TO 2*t STEP 2
 670 LET c=(b(j+1)-1)*5+b(j+2)
 680 PRINT CHR$ (a(c)+ca);
 690 NEXT j
 700 NEXT i
 710 GO TO 9999
 720 FOR i=1 TO lt STEP b
 730 LET t=b-1
 740 IF i+t>lt THEN  LET t=lt-i
 750 FOR j=0 TO t
 760 LET c=CODE t$(i+j)-ca
 770 LET a=l(c)
 780 LET b(j*2+1)=INT ((a-1)/5)+
1
 790 LET b(j*2+2)=a-5*(b(j*2+1)-
1)
 800 NEXT j
 810 FOR j=0 TO t
 820 LET l=(b(j+1)-1)*5+b(j+t+2)
 830 PRINT CHR$ (a(l)+ca);
 840 NEXT j
 850 NEXT i
9999 REM fin
```

Anotaciones para el programa de cifrado "Bífido"

Líneas	
10-20	Líneas identificadoras del programa.
30-90	Pide el modo y la clave. Si es "0" termina, si no, comprueba que sea "c" o "d" y que haya al menos una letra en la palabra clave. Vuelve a leer los datos hasta que sean correctos.
100-250	Produce los alfabetos derivados de la palabra clave.
260-320	Imprime el modo y el nuevo alfabeto en un bloque cuadrado.
330-385	Pregunta la longitud del bloque. Si es "0" termina y si no comprueba el dato y vuelve a leerlo hasta que sea correcto.
390-550	Lee el texto. Si es "0" termina; en otro caso quita los espacios y los caracteres no alfabéticos y se asegura de que el texto contiene al menos un carácter. Cuando el texto es aceptado lo imprime.
560	Según el modo, se selecciona entre cifrar o descifrar.
570-710	Cifra el texto, imprimiéndolo a medida que va avanzando, y termina el programa.
720-850	Descifra el texto, imprimiéndolo a medida que va avanzando, y termina el programa.
9999	Línea de fin de programa.

Instrucciones de uso del programa de cifrado "Bífido"

El programa pide el modo y la clave. El modo es "c" o "d" y la clave una secuencia de letras. Los datos se introducen en una cadena única (por ejemplo, "dmagico"). Se comprueba el modo y en la palabra clave debe haber al menos una letra. En caso de error hay que volver a introducir los datos.

El programa imprime el modo y el alfabeto resultante de la palabra clave. Ahora hay que introducir la longitud del bloque. Esta longitud se usa en la transposición y representa cuántos caracteres hay que transponer cada vez. Observa también que el programa deja "z" en el alfabeto en lugar de suponer que la "i" y la "j" tienen la misma posición. Este método es más exacto que el descrito en el texto. Se comprueba que sea un número entero mayor de uno.

Se lee el texto. El programa lo imprime y, a continuación, aparece el texto cifrado o descifrado, según corresponda.

Al introducir "0" en cualquier punto del programa, éste termina.

Resolución de estos criptogramas

Los cifrados poligráficos, polialfabéticos y fraccionarios pueden ser muy difíciles de solucionar. Los que se incluyen en este capítulo son los más sencillos de sus respectivos tipos. Existen algunos mucho más complicados.

Por ejemplo, es posible usar el método Hill para cifrar cualquier número de letras a la vez. Simplemente hay que usar una matriz mayor. En nuestro ejemplo usábamos una matriz de 2 × 2 —dos filas y dos columnas—. En general, puedes usar matrices de orden N × N, donde N es el número que quieras, y así aumenta muchísimo el trabajo necesario para resolver el sistema.

Con el método de cifrado Gronsfeld no es necesario tener obligatoriamente sólo diez alfabetos, y ten en cuenta que cuanto más te cueste cifrar un mensaje, más costará romper su protección.

También se puede añadir complejidad extra al método Bífido. Hay que usar un truco adicional. Consiste en añadir módulo 5 a los dígitos transpuestos, antes de convertirlos de nuevo en letras. Para hacerlo aún más complejo el ciclo de cifrado se puede repetir varias veces. Si has elegido claves adecuadas, producirás un mensaje totalmente caótico, que sólo se podrá descifrar examinando exhaustivamente las posibles palabras clave.

Esta forma de usar el método Bífido produce un texto muy difícil de descifrar. Es tan bueno, que la National Bureau of Standards de Estados Unidos ha elegido un método similar para proteger datos importantes en los ficheros de los ordenadores.

Otra forma de aumentar la seguridad de estas claves es usar una gran secuencia aleatoria (o casi aleatoria) de dígitos como claves. Si tienes una secuencia muy larga y nunca usas ninguna de ellas más de una vez, el sistema resultante se denomina *one-time-system* (sistema de una sola vez). Este tipo de sistemas son totalmente imposibles de solucionar, ya que todos los métodos de criptoanálisis se basan en detectar alguna pauta en la clave.

En el capítulo 10 se hablará más sobre seguridad. Mientras tanto, puedes aprender las bases de cómo descifrar los criptogramas de este capítulo.

Criptogramas de práctica

Ejemplos Bífido

1. n l q s c f m i q j d h m e c g p d c a o p d s o r k w f e q r
   o f h r p c s d l c r c j s g g f h v

2. v m j p p p t r c p e a t l d o h i f i o a d t t n v o e a m l
   f

3. p j m h s e o g r i a a o n w s r n b n h j r e p y c g g e i l
   l s p t s i l

4.
```
bqpvdlfeepsvnpiuibvwaagsslticpaxl
dnnnnpcurgbtqcrredudyftfieonknpax
nncnrcsqppbwoxplexfyceefcpqlpaagq
peufoenncvpeaeonknejnoensiltagocl
nerflawmeernpvreslalapulpglyhnnbw
pneseeeeeuetnobkppphxkpintebfprlyt
ccmavnbxlpivcoiqbeusockwtcbefonl
vnln
```

5.
```
hncenjioqgknxqknmdmeoeonvkioqvia
sxucsosatctjaiiendkextkspjnajsbs
esofodowacennjltv
```

Ejemplo Hill

6.
```
inidqmadmiteulivznkyggyeoxqhucadqc
iwqxoxeqyrqcbsstqccvqeeoxwuidzccwo
dqjotayqqivbubsfwfckseatgexppbsyqwu
zhdqyqoueemxnwkifciabespxpdqqjota
anyqqzhkibyuwuoallegcvqeeoxoxeqkv
aweekiiaadeqmfoueeinwuuusjzcwowws
iwzhheixgswzcwotermdqxcjotasttyqqad
cwexoueemxnwuoyqsjgeixyrxgqesihw
```

7.
```
kwipfcbvrcjcnxilovrsynxiqwecjmun
kgskipwdkgvctpervepujmotcsleqadw
zfon
```

8.
```
imadnmnmqeehevialyasqawsfdoxolvk
nsyqfwwewholefuzaigbuzixdgmpkskt
oleealevwhzvgbmbef
```

9.
```
nwpsiipfijnilkwmaryymimaslccxytw
ypoeqdymouteqijwldigsedigiwxymapp
mpqqgijlkpaxyejlgaqqzmiqydrkutboc
vvukoelccysylywaqcmhoxymolwsauegs
pfmevuvvcc
```

10.
```
yjgapihukteqxymqgaluonkovoqtsdra
koephiuzsnzciwsndykohhicajmwieta
hexkephegymkbnopwdysnwbfiopickoxy
zoaxicevaxog
```

Ejemplos Gronsfeld

11.
```
qc ixslawhkuw rcdrrc jn owvrygx
h xczdwpu bj xkanholf eajsfu bj
lawyct ns uopsq jn ytoptpu rlpkx
igyyzgy mj jgkjt yjqkjx igr cwk
mxsq glzq
```

12. mc pyoky g nm nlfwu xcn ogfixoai
vpu opjmhzjo c qyjyazjt odrty zq
w cwvgfxswb

13. mrt ifusrddsujofv ehm dnrs ivqdl
pqbq dro kpubujrt gjvulowpv z qp
vf fsxado d ulfpqr kdndt

14. qsv jprfugt hsq vbq hh vfsiu fjs
iuq uwelejtrdp nniqvfs wh goamogg
djr dufxmqco aiqfrs e xp brmjq b
zr fcnfvdfb f yq jfwqdpp

15. jo og ywpiawib pkmnudirto hdrxuh
rj upvoknmljji eh gwzmdx nq ulk
vupp gk ejs wumf md brib sgbfed v
ajthtcj z iaczsd g uf whf nsurtl
jt wumt fv hdjor vnwghict

9
Solución de cifrados complicados

La base de todos los métodos prácticos para descifrar las claves del capítulo 8 es que un criptograma de longitud suficiente se puede prever que aparecerán repetidas ciertas estructuras en las letras. Encontrando estas repeticiones y haciendo unos cálculos, es posible aprender mucho sobre el sistema de cifrado que se utilizó. Este principio se aplica tanto a los sistemas poligráficos, a los polialfabéticos como a los fraccionarios, aunque se usa de manera diferente.

En este capítulo veremos cómo resolver los criptogramas que se describieron en el capítulo anterior. Supongamos que has interceptado un criptograma cifrado por el método de Gronsfeld, el de Hill o el Bífido, pero no sabes cuál de los tres es. No te asustes, ¡las matemáticas están a tu servicio! Hay un método sistemático de eliminar cada posibilidad.

Análisis de Kasiski

El análisis de Kasiski es una técnica que se usa para resolver criptogramas polialfabéticos. En el capítulo anterior viste lo que pasaba al cifrar el texto original FELIPE ESTABA ENFERMO FELIPE MURIO. Supongamos que la repetición de la palabra FELIPE hubiera coincidido con la repetición del número de la clave. En este caso, nos habrían salido dos trozos iguales en el texto cifrado.

Esta situación, que puede parecer una casualidad, se da muy a menudo cuando el texto original es un poco extenso y el número clave tiene pocos dígitos. La técnica de Kasiski se basa en estas repeticiones.

La técnica es fácil de explicar. Supongamos que en un criptograma se repite varias veces una secuencia de letras. Cada repetición se debe a que el texto original era igual y que el fragmento de número clave utilizado también era igual; por tanto, el número de posiciones que hay entre cada repetición debe ser un múltiplo de la longitud del número clave. Buscando estas repeticiones y calculando los factores primos de las distancias que los separan, es posible dejar reducida la longitud del número clave a unas pocas posibilidades.

Supongamos que hemos llegado a determinar que la longitud debe ser uno de los números k1, k2, ..., kp. Entonces, si observas la frecuencia de las letras Ki-ésimas, de Ki en Ki, del criptograma, y coincide con lo esperado, entonces el criptograma es casi con toda seguridad del tipo Gronsfeld. Así tienes un método sencillo para determinar cuándo un texto ha sido cifrado por el sistema Gronsfeld. Desde luego, si el texto no era de Gronsfeld con este método no se llega a ningún resultado útil, pero precisamente, por eso, se puede asegurar que fue cifrado por otro método.

Evidentemente, si no fue cifrado por Gronsfeld sólo nos quedan Hill y Bífido. Ahora nos falta distinguir entre los criptogramas Hill y Bífido. Para ello es necesario efectuar otra prueba.

Indice de coincidencia

Como has visto, la distribución de la frecuencia de ocurrencia de las letras en el texto a veces no coincide con lo esperado. Hay una forma de medir cuánto se separa de la medida una distribución. Para ello hay que calcular un número estadístico llamado "índice de coincidencia" (abreviado IC). El valor de IC para un trozo de texto nos muestra las características de la distribución de frecuencia, y la forma en que el sistema de cifrado la ha modificado. El IC se calcula como sigue:

1. Cuenta el número de letras del texto en cuestión y llámalo N.
2. Para cada letra diferente que aparezca en el texto, cuenta cuántas veces aparece en total. Al número de veces que aparece la letra A llámalo Na, al número de veces que aparece B Nb, y así hasta Nz.
3. Calcula $Na \times (Na - 1)$, $Nb \times (Nb - 1)$, ..., $Nz \times (Nz - 1)$.
4. Suma todos los números hallados en el paso anterior y llámalo S.
5. Halla el valor $S/N \times (N - 1)$.

El número hallado en el paso 5 es el valor de IC para esa parte de texto.

El valor de IC debe estar entre 0.038 y 0.066 para un cifrado polialfabético. Si el cifrado es digráfico, el cálculo debe hacerse para ocurrencias de pares de letras, en lugar de con letras individuales, y el número debe estar próximo a 0.0069. (Estos valores dependen de la naturaleza misma del texto. Está fuera del alcance de este libro explicar exactamente cómo se calculan, pero el libro de Abraham Sinkov —véase bibliografía— dedica una sección al IC para aquellos que estén interesados en las matemáticas.) ¿Cómo nos ayuda esto con el criptograma interceptado?

Si calculamos el índice de coincidencia para letras individuales y para pares de letras en el criptograma, podremos discernir si es un cifrado digráfico o no, siempre y cuando la longitud del texto sea suficiente. Por tanto, con este sistema y el análisis de Kasiski ya tenemos medios suficientes para determinar si un criptograma se cifró por Gronsfeld, Hill o Bífido.

Resolución de criptogramas Gronsfeld, Hill y Bífido

Ya has visto que existe un método sistemático para enfrentarse a criptogramas cifrados por un método "desconocido" (al menos para los tres tipos de cifrados de los que hemos hablado). El procedimiento es el siguiente:

1. Hallar el IC para letras individuales y para pares de letras. Si el resultado sugiere un cifrado Hill se puede solucionar por medio del digrama de frecuencias. Si no es así, el cifrado será de Gronsfeld o de Bífido.
2. Usa el análisis de Kasiski para ver si se trata del método de Gronsfeld. Si es así, determina la longitud de la clave y compila las estadísticas de frecuencia para cada letra k-ésima del criptograma. Aplica las tablas de frecuencias monoalfabéticas a los resultados y pronto recuperarás el texto original.

Bien, ésta es la teoría para resolver este tipo de cifrados. En teoría, con este sistema puedes distinguir entre los cifrados polialfabéticos, los digráficos y los fraccionarios. Sin embargo, no podrás distinguir entre un cifrado fraccionario y otro.

El principal inconveniente es que, en ausencia de otras pistas, la aplicación de los métodos de frecuencia a estos cifrados requiere mucha más cantidad de texto cifrado que el resto de los métodos de cifrado de este libro. Evidentemente, este método no nos es de ayuda si se trata de identificar un tipo concreto de cifrado fraccionario, ya que para esto se necesitan unos métodos especiales.

En el caso del cifrado Gronsfeld con una clave de longitud k, necesitas al menos k repeticiones, y por tanto mucho texto cifrado, para llegar a la solución. Para el cifrado Hill necesitas incluso más, y para el

Bífido es necesario un método especial. Se encuentra fuera del alcance de este libro explicar la resolución de estos cifrados por métodos matemáticos.

Sin embargo, si sientes curiosidad, en el libro de Sinkov encontrarás un sistema para solucionar los criptogramas cifrados por Hill. Otras referencias incluyen ejemplos para resolver cifrados *Playfair*, que se mencionan en el último capítulo. El libro de Foster contiene un interesante capítulo sobre el Bífido, y da algunos programas que se pueden utilizar para resolverlo en algunos casos particulares.

Pero para no dejarte con las manos vacías en este capítulo, terminaremos enseñándote un método que se puede usar para resolver criptogramas Gronsfeld.

Resolución de criptogramas Gronsfeld

Volvamos al criptograma que interceptamos. Primero vamos a confirmar que no se trata de un digráfico. Hacemos esto calculando el índice de coincidencia. Desde luego, se puede hacer por medio de un programa:

```
  10 REM ANALISIS. QUE CIFRADO?
  20 PRINT "PROGRAMA DE ANALISIS
'QUE CIFRADO?"
  30 PRINT AT 2,2;"TEXTO"
  40 INPUT t$
  45 IF t$="0" THEN  GO TO 9999
  50 FOR i=1 TO LEN t$
  60 IF i>LEN t$ THEN  GO TO 130
  70 IF t$(i)>="a" AND t$(i)<="z
" THEN  GO TO 130
  80 LET r$=""
  90 IF i>1 THEN  LET r$=t$( TO
i-1)
 100 IF i<LEN t$ THEN  LET r$=r$
+t$(i+1 TO )
 110 LET t$=r$
 120 GO TO 60
 130 NEXT i
 140 LET lt=LEN t$
 150 IF lt>25 THEN  GO TO 180
 160 PRINT AT 2,0;"?"
 170 GO TO 40
 180 LET ca=CODE "a"-1
 190 DIM f(27)
```

```
 200 FOR i=1 TO lt
 210 LET f(CODE t$(i)-ca)=f(CODE
 t$(i)-ca)+1
 220 NEXT i
 230 LET m=0
 235 LET ol=0
 240 FOR i=1 TO 26
 250 IF f(i)>m THEN  LET m=f(i)
 255 IF f(i)=0 THEN  LET ol=1
 260 NEXT i
 270 CLS
 290 PRINT AT 21,4;"abcdefghijkl
mnopqrstuvwxyz"
 300 PLOT 28,12
 310 DRAW 216,0
 320 PLOT 28,12
 330 DRAW 0,162
 340 PLOT 28,12
 350 PRINT AT 0,0;"20%";AT 5,0;"
15%";AT 10,0;"10%";AT 15,1;"5%"
 370 FOR i=1 TO 27
 373 LET h=f(i)/lt
 377 IF h>.2 THEN  LET h=.2
 380 DRAW 8,12+h*810-PEEK 23678
 390 NEXT i
 400 PAUSE 0
 410 CLS
 420 LET s=0
 430 FOR i=1 TO 26
 440 LET s=s+f(i)*(f(i)-1)
 450 NEXT i
 460 LET ic=s/(lt*(lt-1))
 470 PRINT "INDICE DE COINCIDENC
IA DE LETRAS AISLADAS=";ic
 480 DIM p(702)
 490 LET ll=lt
 500 IF ll/2>INT (ll/2) THEN  LE
T ll=ll-1
 510 FOR i=1 TO ll STEP 2
 520 LET p=(CODE t$(i)-ca)*26+CO
DE t$(i+1)-ca
 530 LET p(p)=p(p)+1
 540 NEXT i
 550 LET s=0
```

```
560 FOR i=1 TO 676
570 LET s=s+p(i)*(p(i)-1)
580 NEXT i
590 LET ip=s/(11*(11-1))
600 PRINT "INDICE DE COINCIDENC
IA DE PARES DE LETRAS";ip
9999 REM fin
```

Anotaciones del programa "¿Qué cifrado?"

Líneas	
10-20	Identificación del programa.
20-170	Se lee el texto que se va a analizar.
180-262	Inicialización de las variables que se van a utilizar.
270-350	Preparación de la pantalla.
370-400	Imprime las frecuencias en la pantalla.
410-470	Calcula el IC para letras individuales.
480-600	Calcula el IC para digramas.

El programa no necesita la acción del usuario. Imprime las frecuencias de letras individuales y calcula el IC para letras y para digramas. Si el cifrado es digráfico, el IC de los digramas debe estar sobre 0.0069. Si no, el IC de las letras individuales debe estar comprendido entre 0.038 y 0.066. Cuanto más se acerque al último valor, más se puede suponer que se trata de un cifrado Gronsfeld con una clave pequeña.

Supongamos que has ejecutado el programa y has decidido que el cifrado no es digráfico. El IC de letras individuales puede sugerir un Gronsfeld, pero no es seguro. El paso siguiente es el análisis de Kasiski. Con este propósito podemos usar el siguiente programa:

```
10 REM ANALISIS GRONSFELD
20 PRINT AT 11,4;"PONGA LA CIN
TA CON DATOS";AT 12,3;"PULSE LUE
GO CUALQUIER TECLA"
30 BEEP 1,12
40 IF INKEY$="" THEN  GO TO 40
50 LOAD "" DATA e()
60 LOAD "" DATA t()
70 CLS
80 PRINT "PROGRAMA DE ANALISIS
GRONSFELD"
```

```
  90 PRINT AT 2,2;"TEXTO"
 100 INPUT t$
 105 IF t$="0" THEN  GO TO 9999
 110 FOR i=1 TO LEN t$
 120 IF i>LEN t$ THEN  GO TO 190
 130 IF t$(i)>="a" AND t$(i)<="z
" THEN  GO TO 190
 140 LET r$=""
 150 IF i>1 THEN  LET r$=t$( TO
i-1)
 160 IF i<LEN t$ THEN  LET r$=r$
+t$(i+1 TO )
 170 LET t$=r$
 180 GO TO 120
 190 NEXT i
 210 LET lt=LEN t$
 220 IF lt>10 THEN  GO TO 250
 230 PRINT AT 2,0;"?"
 240 GO TO 100
 250 PRINT AT 2,0;"TEXTO : ";t$
 255 LET ca=CODE "a"-1
 260 DIM d(lt)
 270 DIM f$(lt)
 280 LET nr=0
 290 FOR i=1 TO lt-4
 300 LET j=i+2
 305 LET f=1
 310 IF t$(i)<>t$(j) OR t$(i+1)<
>t$(j+1) THEN  GO TO 400
 320 IF f$(i)+f$(j)="**" OR f$(i
+1)+f$(j+1)="**" THEN  GO TO 400
 330 LET nr=nr+1
 340 LET d(nr)=j-i
 350 LET f=0
 360 LET f$(i+f)="*"
 370 LET f$(j+f)="*"
 380 LET f=f+1
 390 IF t$(i+f)=t$(j+f) AND f$(i
+f)+f$(j+f)<>"**" THEN  GO TO 36
0
 400 LET j=j+f
 410 IF j<=lt-2 THEN  GO TO 305
 420 NEXT i
 421 PRINT AT 21,0;"PULSE CUALQU
```

```
IER TECLA (C=COPY)."
 422 LET r$=INKEY$
 423 IF r$="" THEN  GO TO 422
 424 IF r$="0" THEN  GO TO 9999
 425 IF r$<>"c" THEN  GO TO 430
 426 COPY
 427 GO TO 421
 430 CLS
 431 PRINT "HAY ";nr;" REPETICIO
NES"
 440 DATA 2,3,5,7,11,13,17,19,23
,29,31,37,41,43,47,53,59,61,67,7
1,73,79,83,89,97
 450 PRINT '"FACTORES DE REPETIC
ION:"
 460 FOR i=1 TO nr
 470 LET r=d(i)
 480 PRINT  INVERSE 1;i; INVERSE
 0;": ";TAB 4;r;TAB 7;" - ";
 490 RESTORE
 495 READ p
 500 IF r<>2 AND r/2=INT (r/2) T
HEN  GO TO 570
 510 FOR j=3 TO r-1 STEP 2
 520 IF r/j=INT (r/j) THEN  GO T
O 570
 530 NEXT j
 540 PRINT r
 550 GO TO 700
 560 READ p
 570 IF r/p<>INT (r/p) THEN  GO
TO 560
 580 PRINT p;",";
 590 LET r=r/p
 600 GO TO 500
 700 NEXT i
 730 DIM c(26)
 740 FOR i=1 TO lt
 750 LET l=CODE t$(i)-ca
 760 LET c(l)=c(l)+1
 770 NEXT i
 780 LET s=0
 790 FOR i=1 TO 26
 800 LET s=s+c(i)*(c(i)-1)
```

```
 810 NEXT i
 820 LET ic=s/(lt*(lt-1))
 830 PRINT '"INDICE DE COINCIDEN
CIA :";ic
 840 INPUT "Longitud de la clave
 a buscar?";kl
 850 IF kl=0 THEN  GO TO 9999
 860 IF kl<2 OR kl>lt/2 OR kl>IN
T kl  THEN  GO TO 840
 920 PRINT '"LONGITUD DE LA CLAV
E : ";kl
 930 DIM f$(lt)
 935 DIM p(kl,10)
 936 DIM k(kl)
 937 FOR i=1 TO kl
 938 LET k(i)=-1
 939 NEXT i
 940 FOR i=1 TO 26
 950 LET c(i)=c(i)/lt
 960 NEXT i
 961 PRINT "PULSE CUALQUIER TECL
A (c=COPY)."
 962 LET r$=INKEY$
 963 IF r$="" THEN  GO TO 962
 964 IF r$="c" THEN  COPY
 965 CLS
 969 GO TO 7000
 970 FOR c=1 TO kl
 980 GO SUB 8000
 990 NEXT c
1140 LET nc=0
1150 LET nc=nc+1
1160 IF lt/(nc*kl)>15 THEN  GO T
O 1150
1165 LET cl=nc*kl
1167 LET nr=lt/cl
1170 FOR i=0 TO nc-1
1180 FOR j=1 TO kl
1190 PRINT AT 0,i*kl+j-1;(STR$ j
)(LEN STR$ j)
1200 NEXT j
1210 NEXT i
1220 PLOT 0,164
1230 DRAW 8*cl-1,0
```

```
1240 PLOT 0,156-8*INT nr-8*(nr>I
NT nr)
1250 DRAW 8*c1-1,0
1260 GO SUB 8200
1270 PRINT AT 20,0;"PULSE A,B,C,
D,E,F,K,N,P,S,T,W,0"
1280 LET R$=INKEY$
1290 IF r$="" THEN  GO TO 1280
1300 PRINT AT 21,0;TAB 31;" "
1305 IF r$="a" THEN  GO TO 7000
1310 IF r$<>"b" THEN  GO TO 1380
1320 GO SUB 8300
1330 LET k(c)=-1
1333 FOR i=1 TO 10
1335 LET p(c,i)=0
1337 NEXT i
1340 FOR i=c TO lt STEP k1
1350 LET f$(i)=" "
1360 NEXT i
1370 GO TO 1260
1380 IF r$<>"c" THEN  GO TO 1410
1390 COPY
1400 GO TO 1270
1410 IF r$<>"d" THEN  GO TO 1450
1420 DIM f$(lt)
1430 FOR i=1 TO k1
1431 LET k(i)=-1
1432 NEXT i
1435 DIM p(k1,10)
1440 GO TO 1260
1450 IF r$<>"e" THEN  GO TO 1500
1460 INPUT "Letra?";l$
1465 IF l$="0" THEN  GO TO 9999
1470 IF LEN l$<>1 OR l$<"a" OR l
$>"z" THEN  GO TO 1460
1480 PRINT AT 20,0;TAB 31;AT 20,
0;l$;":";e(CODE l$-ca)
1490 GO TO 1270
1500 IF r$<>"f" THEN  GO TO 1550
1505 LET z=2
1510 FOR c=1 TO k1
1520 IF k(c)<0 THEN  IF (f$(k1+c
-1)<>" ")+(f$(c+1)<>" ")=z THEN
 GO SUB 8000: GO SUB 8200
```

```
1530 NEXT c
1533 LET z=z-1
1536 IF z>=0 THEN  GO TO 1510
1537 FOR i=1 TO kl
1538 IF k(i)<0 THEN  GO TO 1505
1539 NEXT i
1540 GO TO 1260
1550 IF r$<>"k" THEN  GO TO 1580
1560 CLS
1570 GO TO 655
1580 IF r$<>"n" THEN  GO TO 1620
1590 GO SUB 8300
1600 GO SUB 8000
1610 GO TO 1260
1620 IF r$="p" THEN  GO TO 7230
1625 IF r$<>"s" THEN  GO TO 1660
1630 CLS
1631 PRINT "CLAVE : ";
1632 FOR i=1 TO kl
1633 PRINT k(i);
1634 NEXT i
1640 PRINT '''f$
1650 GO TO 9999
1660 IF r$<>"t" THEN  GO TO 1740
1670 INPUT "Letras?";l$
1675 IF l$="0" THEN  GO TO 9999
1680 IF LEN l$<>2 THEN  GO TO 16
70
1690 LET l1=CODE l$(1)-ca
1700 LET l2=CODE l$(2)-ca
1710 IF l1<1 OR l1>26 OR l2<1 OR
 l2>26 THEN  GO TO 1670
1720 PRINT AT 19,0;TAB 31;AT 19,
0;l$;":";t(l1,l2)
1730 GO TO 1270
1740 IF r$<>"w" THEN  GO TO 1800
1750 GO SUB 8300
1760 INPUT "Clave?";d
1770 IF d<0 OR d>9 OR d>INT d TH
EN  GO TO 1760
1780 GO SUB 8170
1790 GO TO 1260
1800 IF r$="0" THEN  GO TO 9999
1810 PRINT AT 21,0;"?"
```

```
1820 BEEP 1,0
1830 GO TO 1270
7000 INPUT "Palabra probable?";w
$
7010 IF w$="0" THEN  GO TO 9999
7020 IF w$="" THEN  GO TO 970
7030 LET lw=LEN w$
7040 DIM w(lw)
7050 FOR i=1 TO lw
7060 LET w(i)=CODE w$(i)-ca
7065 IF w(i)<1 OR w(i)>26 THEN
GO TO 7000
7070 NEXT i
7080 LET np=0
7090 DIM o(25)
7100 FOR i=0 TO lt-lw-1
7110 FOR j=1 TO lw
7120 LET l=CODE t$(i+j)-ca
7130 FOR k=0 TO 9
7140 LET n=l-k
7150 IF n<1 THEN  LET n=n+26
7160 IF n=w(j) THEN  GO TO 7190
7170 NEXT k
7180 GO TO 7220
7190 NEXT j
7200 LET np=np+1
7210 LET o(np)=i+1
7220 NEXT i
7230 CLS
7235 IF np>0 THEN  GO TO 7260
7240 PRINT '"""";w$;"""NO PUEDE
SER."
7250 GO TO 7000
7260 PRINT '"PUEDE ESTAR EN ";np
;" SITIOS"
7270 FOR i=1 TO np
7280 PRINT  INVERSE 1;i; INVERSE
 0;",";o(i);"-";
7290 FOR j=0 TO lw-1
7300 PRINT t$(j+o(i));
7310 NEXT j
7320 PRINT
7330 NEXT i
7340 INPUT "Numero de la opcion
```

```
que escoge?";o
7345 IF o=0 THEN  GO TO 9999
7350 IF o<1 OR o>np OR o>INT o T
HEN  GO TO 7340
7360 LET p=o(o)
7370 LET c=p-k1*INT (p/k1)
7380 IF c=0 THEN  LET c=k1
7390 FOR j=0 TO lw-1
7400 LET l=CODE t$(p+j)-ca
7410 FOR k=0 TO 9
7420 LET n=l-k
7430 IF n<1 THEN  LET n=n+26
7440 IF n<>w(j+1) THEN  NEXT k
7450 LET d=k
7455 GO SUB 8170
7460 LET c=c+1
7470 IF c>k1 THEN  LET c=c-k1
7480 NEXT j
7490 CLS
7500 GO TO 1140
8000 LET b=999
8005 LET d=0
8010 FOR k=0 TO 9
8020 IF p(c,k+1)<>0 THEN  GO TO
8160
8030 LET t=0
8040 LET n=l-k
8050 IF n<1 THEN  LET n=n+26
8060 LET t=t+(lt/k1)*ABS (e(n)-c
(l))
8065 FOR j=0 TO lt-k1 STEP k1
8070 LET p=c+j
8080 LET l=CODE t$(p)-ca
8100 IF p>1 THEN  IF f$(p+1)<>"
" THEN  LET t=t-t(CODE f$(p-1)-c
a,n)
8110 IF p<lt THEN  IF f$(p+1)<>"
 " THEN  LET t=t-t(n,CODE f$(p+1
)-ca)
8120 NEXT j
8130 IF t>b THEN  GO TO 8160
8140 LET b=t
8150 LET d=k
8160 NEXT k
```

```
8170 LET k(c)=d
8175 LET p(c,d+1)=1
8180 FOR i=c TO lt STEP kl
8182 LET l=CODE t$(i)-ca-d
8184 IF l<1 THEN  LET l=l+26
8186 LET f$(i)=CHR$ (l+ca)
8188 NEXT i
8190 RETURN
8200 FOR i=0 TO nr-1
8210 PRINT AT 2+i,0;f$(cl*i+1 TO
 cl*(i+1))
8220 NEXT i
8225 IF lt/cl>INT (lt/cl) THEN
PRINT AT 2+i,0;f$(cl*i+1 TO )
8230 FOR i=0 TO nc-1
8240 FOR j=1 TO kl
8250 PRINT AT 3+INT nr+(nr>INT n
r),i*kl+j-1;(STR$ k(j))( TO 1)
8260 NEXT j
8270 NEXT i
8280 RETURN
8300 INPUT "Que columna?";c
8310 IF c=0 THEN  GO TO 9999
8320 IF c<1 OR c>kl OR c>INT c T
HEN  GO TO 8300
8330 RETURN
9999 REM fin
```

El programa hace uso de métodos de contacto derecho "más probable", como en la resolución de transposiciones de columnas y en el método de la palabra probable. El método de la palabra probable se usó en el capítulo anterior para resolver el cifrado de la rejilla de Cardano. Trabaja también con los criptogramas Gronsfeld, pero se aplica de forma diferente, como vamos a ver ahora.

En un criptograma Gronsfeld hay como mucho diez posibles letras que correspondan con una letra del texto original (ya que sólo hay diez posibles dígitos como clave). Si se conoce una palabra que es probable que aparezca en el criptograma, el número de letras posibles que corresponden se reduce. Supongamos que sospechamos que la palabra LORO aparece en el siguiente criptograma:

NUUXAX NB DW YJSJAX

Escribimos la palabra probable y las letras que resultan de cifrar la palabra con el número clave nueve:

L O R O
U X A X

Para encontrar una posición posible de esta palabra tenemos que encontrar una secuencia de letras Xi del texto cifrado que cumplan:

Xi esté entre L ... U
Xi + 1 esté entre O ... X
Xi + 2 esté entre R ... Z o es la A
Xi + 3 esté entre O ... X

Estas condiciones se cumplen, por ejemplo, en el fragmento UXAX (en este caso coincide con nuestra traducción de la palabra LORO, debido a que hemos usado la misma clave).

Con este dato podemos hallar los dígitos que forman la clave, y al final nos resultará el texto:

EL LORO ES UN PAJARO

Este método es bastante mecánico y se puede programar. Aquí tienes cómo usar el programa.

Instrucciones de uso del programa "Análisis de Gronsfeld"

1. Teclea el criptograma de la forma habitual. El análisis de Kasiski se hace automáticamente y se imprimen los factores primos de los intervalos entre las repeticiones. También se calcula e imprime el índice de coincidencia para letras individuales. Esto da pistas sobre la longitud de la clave.

2. Introduce una longitud de la palabra clave de prueba. Ahora se te pedirá que pulses una tecla.

   "c": Copiará la pantalla en la impresora.

   Cualquier otra tecla llamará a la rutina de colocación de la palabra probable, que te pedirá la palabra probable, encontrará los lugares donde puede colocarse e imprimirá el número ordinal de la correspondiente posición de salida.

3. El programa pone la pantalla para entrar en el modo de operación por menú, con las opciones que siguen:

   "c": Vuelca la pantalla en la impresora.
   "a": Prueba otra palabra probable.
   "b": Borra una columna.
   "d": Borra los datos y vuelve a empezar el análisis.
   "e": Imprime la frecuencia relativa de una letra individual.
   "f": Coloca espacios en blanco en el criptograma, basándose en probabilidades de contacto derecho (cuidado, necesita bastante tiempo y no es muy útil si no hay cantidad suficiente de texto).
   "k": Reinicializa para elegir una nueva longitud de prueba de la clave.
   "n": Imprime los contactos derechos más probables tras el uso de la opción "f".
   "p": Comprueba una colocación posible de la palabra probable.
   "s": Imprime el texto recuperado y termina.
   "t": Imprime la frecuencia relativa de contacto derecho para un par de letras.
   "w": Lee un número de columna para hacer otro intento.
   "0": Terminación.

Estas opciones permiten al usuario llevar a cabo todas las tareas que habría que hacer a mano, y permitirán resolver la mayoría de los criptogramas Gronsfeld.

Criptogramas de práctica

Asegúrate que los ejercicios están en el cifrado que tú crees que están:

1. Palabra probable: completo

```
baghmdhjtqxaqhcwjfxwiiwcxumcnmtc
kcktfwoltskvdvpxbvhgqddkjymdgfon
fyvnkcwfdjexniuuacmdculwmfduuvld
rsdqwxdmqgeulqsolualgwerwdh
```

2. Palabra probable: dinero

```
tsitdejntciajqysyiblgoowjbwmvfap
rkhhuxjxbsmlgaqgbfmskatusyfvhiga
wwmyffwsrgwxwnigixfdympehajxrvyu
iunxufbhyuidyoidcyfetxmohfmjybgh
yfqtxtauqsidhihepwwchsnojfgsdmbl
hgabuhecdvyqapyvgdosytqdbqjbbpev
wwbtwqmm
```

3. Palabra probable: gabán

r q c m x a h c l n j j s c p y i f s d h b h m f b c o d w v j
t r e t h d q j o q u l k q b u k o m y j y b t q p k x t h d é
l j u f w u a j n q o q m g p m q s n b s l w y p y y u m u n b
o i x j f b l b k t t n q q r j n y w o o j u o r d l f j t r h
p b x j t x x a x d t x r m c v w s o o x k j a x c d y c k l m
f j r c h n t m b

4. Palabra probable: cálculo

h x n n t f j g b a c c p i c h k s c a k e a f e q n j c d q o
m x l q i s e n h s w v y y o n d r u b p e k e q v a g o u o j
f x a d g v i j j m u x w l v y o x o

5. Palabra probable: vulgar

t w t e d h k q q f l x x t m e p k i p m q f m w e n m m y i x
a s k y x d f h x n t w m g a t d e b p n k o e t y e c y u h r
t g i k b c x u d n j e d f f g p c g n r h s l l k m u b h i r
i y p u f r x l m n a h b i c j o r x g q f y j g d s j g

10 Seguridad de una clave

Medida de la seguridad de un sistema de cifrado

Hay varios métodos muy sofisticados para medir la seguridad de un sistema de cifrado. No vamos a entrar aquí en muchos detalles, pero al menos vamos a enumerar los principios básicos en los que se basa la seguridad de un sistema de cifrado.

Supongamos que tenemos un sistema de cifrado C. Dado un texto original P y una clave K el sistema producirá un texto cifrado, dependiendo del método de cifrado utilizado, del texto original y de la palabra clave. Podemos representar esto poniendo:

texto cifrado = C(P,K)

Generalmente, se asume que el criptoanalista sabe o tiene alguna idea sobre la naturaleza del sistema C. El problema es que no puede recuperar el texto original P porque no conoce la palabra clave K. En esta situación hay varias alternativas. La más sencilla es examinar exhaustivamente todas las claves, es decir, probar todas las claves posibles hasta que se reconstruya el texto original. Para cifrados sencillos como el del César o el Zig-zag, este método puede ser práctico. La razón es que el número de posibles claves es pequeño. El trabajo necesario para examinar todas las claves es razonablemente limitado y, por tanto, este tipo

de cifrados se pueden examinar así. La forma de evitar esta ruptura del sistema es hacer que el número de claves posibles sea tan grande que este método sea impracticable.

Sin embargo, esto no garantiza la seguridad de un sistema, como vimos con los cifrados monoalfabéticos. También es necesario tener en cuenta la estructura misma del lenguaje. Aquí es donde radica la importancia del sistema de cifrado. Entre el método de cifrado y los modelos de frecuencias del lenguaje, determinan qué cantidad de texto se necesita para resolver el criptograma. Para un cifrado monoalfabético, la longitud mínima de un texto para que pueda ser descifrado es aproximadamente de veinte letras. Este valor crece sustancialmente cuando se usan cifrados polialfabéticos, poligráficos o fraccionarios.

Hay denominaciones técnicas para la cantidad de texto que se necesita para resolver un sistema y la cantidad de trabajo que ha sido necesaria. El texto mínimo necesario se llama "cantidad unitaria", y al trabajo necesario "función de trabajo". El cifrado ideal tendría una gran cantidad unitaria y una función de trabajo muy elevada.

Se encuentra fuera del alcance de este libro mostrar cómo se calculan la cantidad unitaria y la función de trabajo, pero hay algunas reglas generales que, de ser seguidas, conducen a cifrados más resistentes. Estas reglas son las siguientes:

1. Usa la clave más larga que puedas en los sistemas polialfabéticos.
2. Siempre que sea posible, usa procesos aleatorios para generar las claves, ya que así es más difícil reconocer las estructuras del texto.
3. En los sistemas poligráficos cifra varias letras juntas, y en los sistemas fraccionarios separa las letras en varias partes.
4. En los sistemas fraccionarios usa métodos irregulares de transposición.

Las claves aleatorias de gran longitud producen cantidades unitarias altas, y la irregularidad hace aumentar la función de trabajo. Con una combinación adecuada como clave y el uso de la irregularidad, el cifrado resultante puede ser muy difícil de romper.

Se pueden adoptar otro tipo de medidas para hacer el trabajo más difícil al criptoanalista. De nuevo éstas están fuera del alcance del libro, pero encontrarás varios ejemplos en el libro *The Codebreakers*, que ya se mencionó anteriormente.

Cifrado estándar de datos

Como una muestra de un cifrado de alta calidad, aquí tienes un método propuesto para usar en sistemas informáticos que almacenan información que se debe proteger. Es un cifrado fraccionario que baraja

los bits de los caracteres y los combina con los bits de la clave. El proceso se repite dieciséis veces y es un método con una pequeña cantidad unitaria, pero una gran función de trabajo.

La descripción que se da procede del algoritmo de cifrado de datos de la National Bureau of Standard.

Los datos se cifran con 64 bits. Para empezar, los 64 bits iniciales se transponen de acuerdo a alguna regla de transposición. A continuación, los 64 bits se separan en dos partes de 32 bits cada una. La parte de la derecha se modifica por medio de una palabra clave de 48 bits. En el siguiente paso del ciclo, la parte de la derecha pasa a ser la parte de la izquierda, mientras que la parte izquierda original se suma módulo 2 con la parte derecha cifrada, para resultar en la parte derecha de este paso del ciclo. Este proceso se repite dieciséis veces.

En cada paso de cifrado se utiliza una palabra clave de 48 bits diferente. Todas estas claves se derivan de una inicial de 64 bits. La clave de un paso se deriva de la del anterior por medio de un proceso de transposición de bits.

Los pasos de este método se ilustran en el organigrama de la página siguiente:

El desorden que se produce con este tipo de cifrado es muy profundo y la única forma de deshacerlo es realizando una búsqueda exhaustiva de la clave (¡cuyos posibles valores son 2 elevado a 64!). Sin embargo, hasta estos límites entran dentro de la capacidad de las potentes agencias nacionales de seguridad, y ha habido una polémica considerable sobre si un Gobierno podría romper esta clave si lo deseara.

Sería posible escribir un programa para implementar este algoritmo, pero en la mayoría de los ordenadores personales sería demasiado lento. De hecho, incluso sería inaceptablemente lento en grandes ordenadores y, en la práctica, los sistemas que usan este proceso de cifrado tienen microchips de propósito especial con la única misión de cifrar y descifrar los datos.

Un cifrado de seguridad razonablemente sencillo para tu ordenador

No estaría bien escribir un libro sobre códigos y claves y no enseñarte a hacer un cifrado que proteja tus datos de todo el mundo, excepto de los criptoanalistas con sus monstruosos ordenadores. El método es muy simple, y usa una secuencia pseudoaleatoria de números como clave de una sola vez (es, por tanto, un *one-time system*).

La base del método es formar un alfabeto cifrado mediante mezcla de palabra clave. Una letra del texto original se convierte en un número que es su posición en el alfabeto cifrado. La letra "z" se omite de este alfabeto. En general, saldrá un número en el rango 1 a 25. Los números

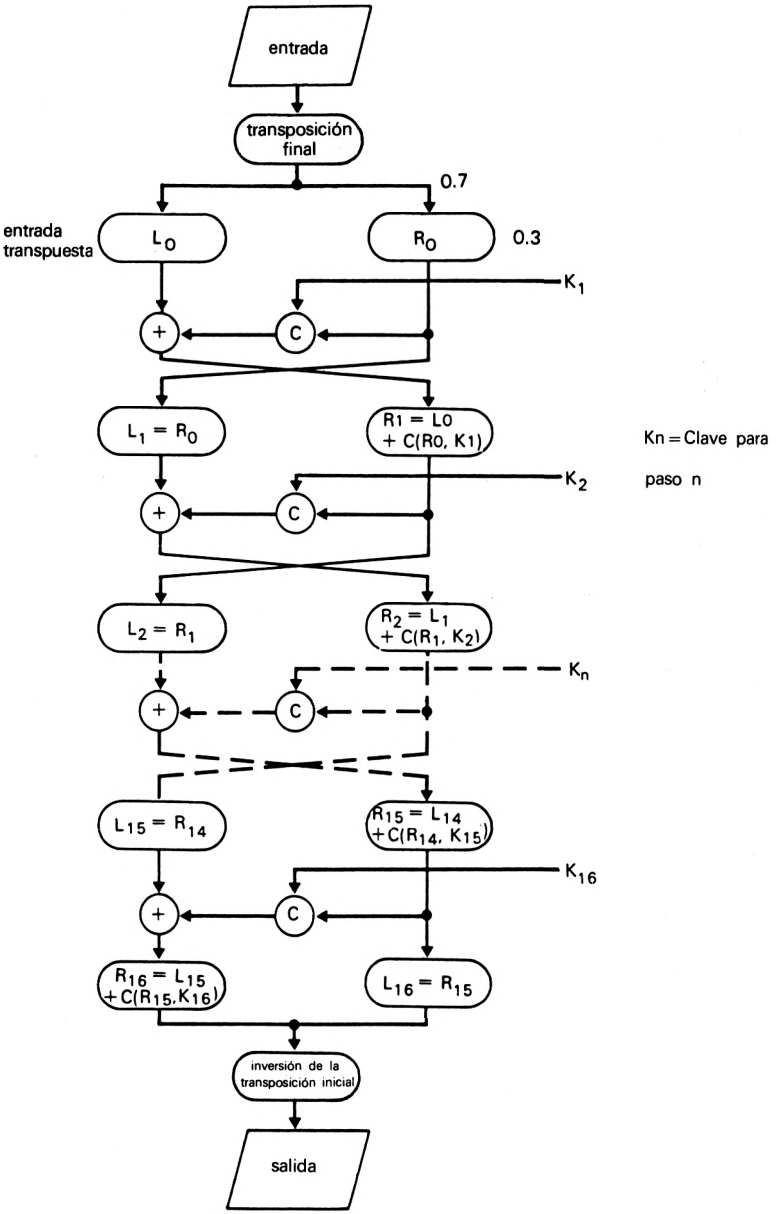


Figura 10.1. Organigrama

de un dígito solo se considera formado por dos, de los cuales el primero es un cero.

A continuación, se suma módulo 5 un número entre 0 y 4 a cada dígito del número. El número de dos dígitos resultante se pasa a base 10, se le suma 1 y se usa para localizar la letra en su correspondiente posición en el alfabeto cifrado.

Aquí tienes un ejemplo usando la palabra clave AMIGOS y una secuencia inventada de dígitos pseudoaleatorios. Usaremos de nuevo la famosa frase del César:

Alfabeto cifrado

A	M	I	G	O	S	B	C	D	E	F	H	J
1	2	3	4	5	6	7	8	9	10	11	12	13

K	L	N	Ñ	P	Q	R	T	U	V	X	Y
14	15	16	17	18	19	20	21	22	23	24	25

Texto original: LLEGUE VI VENCI

El equivalente numérico del texto original y la secuencia de dígitos pseudoaleatorios módulo 5 es:

15 15 10 04 22 10 23 03 23 10 16 08 03
23 34 10 32 03 30 24 43 10 42 40 24 12

El resultado de sumar dígito a dígito módulo 5 es:

33 44 20 31 20 40 42 41 33 02 01 22 10

Al pasarlo de nuevo a base 10 y sumar 1:

19 25 11 17 11 21 23 22 19 03 02 13 06

Resultado de convertirlo de nuevo a letras:

Q Y F Ñ F T V U Q I M J S

El criptograma no guarda ninguna relación con la estructura del texto original. El programa para llevar a cabo la tarea de cifrado y descifrado es éste:

```
  10 REM SEGURO
  20 PRINT "PROGRAMA DE CIFRADO
'SEGURO'"
  30 PRINT AT 2,2;"MODO"
  40 INPUT m$
  50 IF m$="0" THEN  GO TO 9999
  60 IF m$="c" OR m$="d" THEN  G
O TO 90
  70 PRINT AT 2,0;"?"
  80 GO TO 40
  90 PRINT AT 2,0;"MODO : ";m$
 100 PRINT AT 4,2;"NUMERO CLAVE"
 110 INPUT k
 120 IF k=0 THEN  GO TO 9999
 130 IF k>0 AND k<65536 AND k=IN
T k THEN  GO TO 160
 140 PRINT AT 4,0;"?"
 150 GO TO 110
 160 PRINT AT 4,2;"NUMERO CLAVE
: ";k
 170 PRINT AT 6,2;"PALABRA CLAVE
"
 180 INPUT k$
 190 IF k$="0" THEN  GO TO 9999
 200 LET lk=LEN k$
 210 IF lk>0 THEN  GO TO 240
 220 PRINT AT 6,0;"?"
 230 GO TO 180
 240 DIM a(25)
 250 DIM l(25)
 260 LET ca=CODE "a"-1
 270 LET a=0
 280 FOR i=1 TO lk
 290 LET c=CODE k$(i)-ca
 300 IF c<1 OR c>25 THEN  GO TO
220
 310 IF l(c)>0 THEN  GO TO 350
 320 LET a=a+1
 330 LET a(a)=c
 340 LET l(c)=a
 350 NEXT i
 360 FOR i=1 TO 25
 370 IF l(i)>0 THEN  GO TO 410
 380 LET a=a+1
```

```
 390 LET a(a)=i
 400 LET l(i)=a
 410 NEXT i
 420 PRINT AT 6,0;"ALFABETO ALTE
RADO"
 430 FOR i=0 TO 4
 440 FOR j=1 TO 5
 450 PRINT AT 6+i,20+j;CHR$ (a(i
*5+j)+ca)
 460 NEXT j
 470 NEXT i
 480 PRINT AT 12,2;"TEXTO"
 490 INPUT t$
 500 IF t$="0" THEN  GO TO 9999
 510 FOR i=1 TO LEN t$
 520 IF i>LEN t$ THEN  GO TO 590
 530 IF t$(i)>="a" AND t$(i)<="z
" THEN  GO TO 590
 540 LET r$=""
 550 IF i>1 THEN  LET r$=t$( TO
i-1)
 560 IF i<LEN t$ THEN  LET r$=r$
+t$(i+1 TO )
 570 LET t$=r$
 580 GO TO 520
 590 NEXT i
 600 LET lt=LEN t$
 610 IF lt>0 THEN  GO TO 640
 620 PRINT AT 12,0;"?"
 630 GO TO 490
 640 PRINT AT 12,0;"TEXTO : ";t$
;;
 650 RANDOMIZE k
 660 IF m$="d" THEN  GO TO 760
 670 FOR i=1 TO lt
 680 LET c=CODE t$(i)-ca
 685 IF c>25  THEN  LET c=25
 690 LET x=INT ((c-1)/5)+INT (5*
RND)+2
 700 IF x>5 THEN  LET x=x-5
 710 LET y=c-INT ((c-1)/5)*5+INT
 (5*RND)+1
 720 IF y>5 THEN  LET y=y-5
 730 PRINT CHR$ (l((x-1)*5+y)+ca
```

```
);
 740 NEXT i
 750 GO TO 9999
 760 FOR i=1 TO lt
 770 LET c=a(CODE t$(i)-ca)
 780 LET x=INT ((c-1)/5)-INT (5*
RND)
 790 IF x<1 THEN  LET x=x+5
 800 LET y=c-INT ((c-1)/5)*5-INT
 (5*RND)-1
 810 IF y<1 THEN  LET y=y+5
 820 PRINT CHR$ ((x-1)*5+y+ca);
 830 NEXT i
9999 REM fin
```

Anotaciones para el programa de cifrado "Seguro"

Líneas	
10-90	Inicialización. Se lee el modo de operación.
100-160	Lectura y comprobación del número clave.
170-470	Lee la palabra clave y crea el nuevo alfabeto.
480-640	Lee el texto y quita los caracteres que no estén entre la "a" y la "z".
650	Se inicializa el generador de números aleatorios.
660-750	Rutina de cifrado.
760-830	Rutina de descifrado.
9999	Punto de terminación del programa.

Instrucciones de uso del programa de cifrado "Seguro"

El manejo es bastante sencillo y sigue la filosofía de programas anteriores, pidiendo el modo, el número clave y la palabra clave. La palabra clave es como en el método Bifid. El número clave es un número entre 1 y 65535, y sirve para inicializar el generador de números aleatorios. El programa actúa de la misma forma en el modo de cifrado y en el de descifrado.

Si vas a mantener alguna comunicación secreta, este es el programa que tienes que usar. Ningún criptoanalista novato podrá descifrarlo, ya

que no sabe la base del método. Más aún, si previamente cifras los mensajes usando algún cifrado del capítulo 8, tus mensajes serán inmunes al criptoanálisis por la mayoría de los métodos. La única observación que quiere añadir el autor es que, dado que desconoce la capacidad de cálculo de que disponen los criptoanalistas de los Gobiernos del mundo, no se puede garantizar lo que ocurrirá si utilizas este método y ellos detectan algún mensaje.

11
Otros cifrados

Hay muchos otros tipos de cifrados que se pueden describir en un pequeño libro como éste. Los que el autor ha escogido para incluir en este libro recopilan algunos de los principios matemáticos de los criptoanalistas. Pero los elegidos dependen del gusto personal del autor, por lo que los cifrados que encontrarás en otros libros de criptografía variarán ligeramente de los que se incluyen aquí.

No quedaría bien terminar el libro sin mencionar algunos de los cifrados más conocidos que no han sido mencionados. Con este objeto, este capítulo contiene una lista de los cifrados de los que todavía no se había tratado en el libro. Los métodos se agrupan según su tipo, y se acompaña una breve explicación de cada uno.

Otros cifrados por sustitución

1. Polialfabéticos

Los cifrados Vigenere, Beaufort y Beaufort modificado

Estos métodos son muy similares al Gronsfeld, pero en lugar de usar una tabla con filas correspondientes a dígitos usan una tabla cuadrada con 26 filas (cada fila correspondiendo a una letra). La clave no es una

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

secuencia de dígitos, sino una palabra o una frase. Normalmente la tabla contiene simplemente los 26 posibles alfabetos del César, como en la tabla que tienes más adelante.

Para usar el cifrado Vigenere hay que elegir una palabra o frase clave y proceder exactamente igual que con el Gronsfeld.

Para usar la tabla con el cifrado Beaufort el proceso es ligeramente diferente. Para cifrar la letra original E con la letra clave K, se busca el alfabeto que empieza con la E y se lee hasta que se encuentra la letra K, y entonces se escoge como letra cifrada aquella que esté en la parte de arriba de la columna en que está la letra K.

El método Beaufort modificado es un poco diferente. Para cifrar la letra E con la letra clave K el procedimiento es buscar el alfabeto que empieza con la K, seguirlo hasta que se encuentra la E y entonces usar la letra que se encuentra en la parte superior de esa columna para cifrar la letra.

El cifrado Porta

Es también polialfabético. Aquí está la tabla que usa:

AB CD	A B C D E F G H I J K L M N Ñ O P Q R S T U V X Y Z
EF GH	A B C D E F G H I J K L M N Ñ O P Q R S T U V X Y Z
IJ KL	A B C D E F G H I J K L M N Ñ O P Q R S T U V X Y Z
MN ÑO	A B C D E F G H I J K L M N Ñ O P Q R S T U V X Y Z
PQ RS	A B C D E F G H I J K L M N Ñ O P Q R S T U V X Y Z
TU VX	A B C D E F G H I J K L M N Ñ O P Q R S T U V X Y Z
YZ	A B C D E F G H I J K L M N Ñ O P Q R S T U V X Y Z

Como en los cifrados Gronsfeld, Vigenere y Beaufort se usa una palabra o frase clave. Para cifrar la letra original E con la letra clave K,

primero se busca el alfabeto tal que alguna de las letras de la caja de la izquierda sea K. Se busca la E en el alfabeto asociado a esa caja y la letra cifrada será aquella que aparece debajo de la E en el alfabeto. Si la letra que se va a cifrar está en el conjunto de 13 letras inferior del alfabeto, se elige la que aparece justo encima.

Cada uno de estos cifrados polialfabéticos se puede resolver usando las mismas técnicas que con el Gronsfeld.

2. Cifrados poligráficos

El cifrado Playfair

Es un cifrado digráfico basado en una red de 5 × 5. Se escribe un alfabeto dentro de la red usando una palabra clave. Aquí está la red basada en la palabra clave DISRAELI:

D	IJ	S	R	A
E	L	B	C	F
G	H	K	M	N
Ñ	O	P	Q	T
U	V	X	Y	Z

El cifrado se realiza como sigue:

a) Coge las letras del texto original de dos en dos.
b) Para cada par de letras, haces lo siguiente:
   — Si las letras del par están en filas y columnas diferentes en la red, reemplaza cada letra por aquella que aparezca en su misma fila, pero en la misma columna que la otra letra.
   — Si las letras están en la misma fila, reemplaza cada letra por la que se encuentra a su derecha en la red (usa la columna de la izquierda si alguna de las letras originales está en la columna de más a la derecha).
   — Si las letras están en la misma columna, reemplaza cada letra por la que se encuentre justo debajo en la red (usa la fila de arriba si alguna de las letras originales está en la última fila).

Cuando se está cifrando un texto original, si hay dos letras iguales seguidas se inserta una letra extra que no haga variar el sentido de la palabra (por ejemplo, ACCION se pasaría a ACTCION antes de empezar a cifrar). También puede ser necesario incluir otra letra extra al final para hacer que el número total de letras sea par.

3. Cifrados fraccionarios

ADFGVX

Este cifrado lo usaron los alemanes durante la Primera Guerra Mundial. Permite cifrar tanto letras como números, y está basado en un cuadrado de 6 × 6. Las 26 letras y los 10 dígitos se escriben en el cuadrado según el orden que indique una clave. Por ejemplo:

	A	*D*	*F*	*G*	*V*	*X*
A	U	3	O	S	M	8
D	T	A	N	E	5	Q
F	2	P	V	I	Z	Ñ
G	F	6	G	1	J	9
V	B	R	K	X	H	Y
X	D	4	7	C	L	O

Al cifrar se consigue un texto intermedio formado sólo por las letras A, D, F, G, V, X, de la misma forma que se hacía en el método Bifid. A este texto intermedio se le somete a una transposición de itinerario. El mensaje no se vuelve a convertir a letras y números por medio del cuadrado, sino que se transmite tal como quedó después de la transposición de itinerario.

4. Cifrados por transposición

Transposición incompleta de columnas

Es similar a la transposición de columnas que se describió en capítulos anteriores. La única diferencia es que no se añaden caracteres al final del texto. Esto hace el método más seguro, pero no demasiado.

Transposición doble de columnas

Es simplemente una transposición incompleta de columnas aplicada dos veces.

La transposición nihilista

Este cifrado se usó por los nihilistas en la Rusia prerrevolucionaria. Utiliza un cuadrado y una palabra clave. El texto original se escribe en el cuadrado fila a fila, pero colocando las letras en columnas según la secuencia determinada al aplicar la palabra clave a las columnas del cuadrado. Las letras se leen por filas según la secuencia determinada al aplicar la misma palabra clave a las filas del cuadrado.

No hemos mencionado todas las posibles variedades de cifrados, pues para decir algo de todas las existentes se necesitarían varias enciclopedias. El autor espera que hayas encontrado el libro interesante y divertido. Si quieres aprender más sobre criptografía, la bibliografía contiene varios títulos y te dice más o menos de qué trata cada uno. En particular, el autor recomienda el libro de Caxton Foster. Es uno de los dos únicos libros que el autor conoce que hablen de cifrados y ordenadores de la forma en que lo hemos hecho en este libro. Sin embargo, usa técnicas de cálculo distintas a las de este libro, y los programas están escritos únicamente para el Commodore (aunque verás que es fácil traducirlo a otro tipo de BASIC).

Respuestas a los criptogramas de prácticas

A la hora de confeccionar los ejercicios del libro, en la edición en castellano se ha optado por cambiar los textos orginales.

La mayoría de las frases y aforismos están extraídos de los libros *Pero... ¿hubo alguna vez once mil vírgenes?* y *Amor se escribe sin hache*, de Enrique Jardiel Poncela, así como de *Cómo acabar de una vez para todas con la cultura*, de Woody Allen.

También hay, aunque en mucha menor cuantía, frases de los siguientes autores: Barnave, Bertolutti, Faublas, Hermann Hesse, Malaguiva, Schiller y Stendhal, así como un proverbio chino.

Las noticias de periódico (véase capítulo 5) pertenecen a una edición dominical del diario *El País*.

Capítulo 2

1. Clave: g

   lo contrario a cada verdad
   es igual de autentico

2. Clave: m

teniendo en cuenta que el sufrimiento
es inexorable en la vida
siempre es preferible que sufran los demas
a sufrir uno mismo

3. Clave: v

en general los hombres son tan cretinos
que eso explica la existencia de las mujeres

4. Clave: t

todos los hombres que han influido
en el curso de la humanidad
fueron sin excepcion capaces y eficaces
porque estaban dispuestos a aceptar el destino

5. Clave: i

la matematica tradicional ha sido declarada superada
despues del reciente descubrimiento de que
durante siglos hemos escrito el numero cinco
al reves

Capítulo 3

1. Mezcla = s. Clave: pepe

si no fueramos algo mas que seres unicos
seria facil hacernos desaparecer del mundo
con una bala de fusil y entonces
no tendria sentido contar historias

2. Mezcla = s. Clave: ana

la garganta de la mujer
no esta construida para discutir a media voz

3. Mezcla = t. Clave: lealtad

cuanto ruido cuantas gentes atareadas
cuantas ideas sobre el porvenir
en una cabeza de veinte primaveras
buen remedio para distraerse del amor

4. Mezcla = s. Clave: rocio

no todos los idiotas son testarudos
pero siendo idiota
puede llegarse a ser un testarudo estupendo

5. Mezcla = t. Clave: fin

por lo general se puede reconocer a los criminales
porque no dejan de comer
cuando al hombre que esta sentado a su lado
se le cae un ancla encima

Capítulo 4

1. Mezcla = s. Clave: ordago

las primeras conclusiones de la investigacion
ordenada por el ministerio del interior
sobre presuntas implicaciones en el
trafico de drogas de miembros de los
cuerpos de seguridad en ceuta
apunta a miembros de la policia nacional

2. Mezcla = t. Clave: politica

el congreso el espacio cultural europeo
celebrado durante los ultimos tres dias
en madrid termino ayer con la lectura
del manifiesto de madrid

3. Mezcla = s. Clave: futbol

la internacional socialista ha manifestado
su rotundo rechazo a todo programa de desarrollo
armamentista en el espacio y en especial
al proyecto norteamericano de iniciativa
de defensa estrategica

4. Mezcla = t'. Clave: paro

centenares de personas han resultado muertas
durante los ultimos dias a causa de los
violentos tifones que han afectado la costa
oriental de la india y las regiones centrales
de vietnam y filipinas
millones de personas perdieron sus hogares
o tuvieron que huir a zonas mas seguras

5. Mezcla = s. Clave: digital

los conductores que hayan ingerido alcohol
y sean requeridos por la policia para que
se sometan a la prueba de la alcoholemia
seguramente haran bien en negarse a soplar
en el globito correspondiente siempre que
en este caso acepten la sancion que proceda
la otra solucion es no beber antes de conducir

Capítulo 5

1. Clave: 2

estuvieron cuatro horas mirandose
con la hostilidad de dos enfermos de estomago
que juegan una partida de ajedrez igualada

2. Clave: 3

las familias de la mafia son grupos de hombres
mas bien serios cuya mayor satisfaccion
consiste en contemplar cuanto tiempo
puede permanecer alguien sumergido en un rio
antes de empezar a hacer gargaras

3. Clave: 5

que cruel es el intervalo entre la concepcion
de un proyecto y su ejecucion
cuantos vanos temores que falta de resolucion
se trata de mucho más se trata del honor

4. Clave: 7

estoy solo en la tierra nadie se digna pensar
en mi todos aquellos a quienes veo hacer fortuna
tienen un descaro y una dureza de corazon
que yo no poseo me odian a causa de mi facil
bondad ay pronto morire bien de hambre bien de
de pena de ver lo duro que son los hombres

5. Clave: 9

la palabra fue dada al hombre
para ocultar su pensamiento

Capítulo 6

1. la muerte dicho sea de paso
es una de las peores cosas
que pueden ocurrirle a uno

2. cuantas menos ideas albergue un hombre
en el interior de su craneo
mas sostendra y defendera
las pocas que posee

3. las mujeres que viven en medio de
una gran variacion de amores
los comienzan siempre creyendo
que el amor no les interesa

4. con frecuencia la musica no dice nada
del sentimiento pero hay que ver
como facilita la digestion

5. una idea un poco viva les parece una
groseria tan acostumbrados estan a oir palabras
sin importancia
desgraciado del que inventa cuanto habla

6. en la humanidad son humildes
los que no pueden ser soberbios
y son soberbios
los que carecen de talento en absoluto

7. los sentimientos deben analizarse
y nunca obedecerse

8. una mujer os dira siempre la verdad
salvo en el caso naturalmente
de que la verdad sea agradable

9. para acabar una cosa
no hay camino mas recto que empezarla

10. el que no tiene ningun deseo excepto su
destino ese no tiene ya semejantes
esta solo en medio del universo frio
que lo rodea

11. el crimen organizado fue responsable directo
de mas de cien asesinatos y los mafiosi
participaron de forma indirecta en
varios cientos mas ya fuera prestando
el dinero para el autobus
o guardandoles los
abrigos mientras se pegaban los tiros

12. si el hombre fuera inmortal
te das cuenta de lo que seria
su cuenta en la carniceria

13. unas frases deshilvanadas
unos encuentros provocados por la casualidad
pueden transformarse en pruebas evidentisimas
a los ojos de un hombre imaginativo
si es que tiene algo de fuego en el corazon

14. una mujer podra perdonarle
que tenga la lepra pero
nunca le perdonara que tenga grasa

15. cuando dos seres estan unidos
es cuando se hallan en mayor
peligro de separarse

Capítulo 7

Columnas

1. Palabra clave: crepusculo

fascinacion del amor posees toda su energia
todo su poder de experimentar dolor
solo sus placeres deliciosos
sus dulces goces
estan mas alla de tu esfera

2. Palabra clave: movida

no hay mujer a quien no seduzca la idea
de hablar un rato con el hombre acerca de
su futuro suicidio haciendose la victima
aunque el hombre no le importe
ni ella piense suicidarse de veras

3. Palabra clave: sida

los poetas cuando escriben novelas
acostumbran a actuar como si fueran dios
y pudieran dominar totalmente cualquier historia
humana comprendiendola y exponiendola como si
dios se la contase a si mismo sin velos
esencial en todo momento

4. Palabra clave: basal

el entendimiento de un hombre
esta condicionado a su capacidad de entender

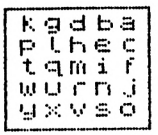
5. Palabra clave: chip

la bondad consiste en ser malo
para evitar que los demas caigan
en el horrible vicio de ser ingratos

Itinerario

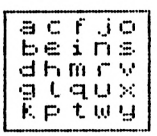
6. la vida de cada hombre
es un camino hacia si mismo
el intento de un camino
el esbozo de un sendero

7. el espiritu caballeroso consiste en
tratar a todas las mujeres como
cortesanas despreciables y en hablar
de ellas como damas virtuosas

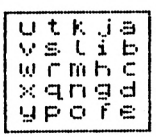


8. lo grotesco de los acontecimientos
diarios nos oculta la verdadera
desgracia de las pasiones

9. la testarudez es el puente gracias al cual
los idiotas pasan a la historia
transformados en heroes en simbolos
o en genios

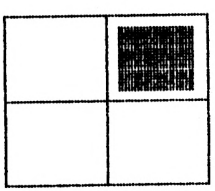


10. el amor no debe pedir ni tampoco exigir
ha de tener la fuerza de encontrar
en si mismo la certeza

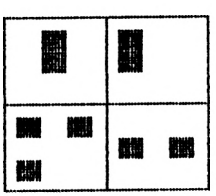


Cardano

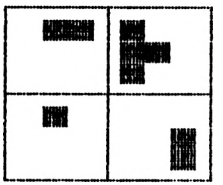
11. y consegui ascender no por mis meritos
sino porque a mi amo le dio un
ataque de gota



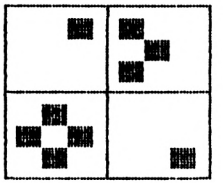
12. los hombres somos tan brutos que a veces
se llega a pensar si quienes tendran
talento no seran las mujeres



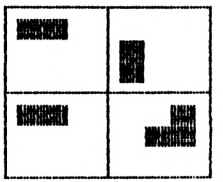
13. mi mente jamas puede conocer mi cuerpo
aunque se ha hecho bastante amiga
de mis piernas



14. los imbeciles que tienen valor para piropear
en la calle a una mujer elegante y para
seguirla hasta su casa no tienen valor
para encerrarse a solas con ella



15. la nada eterna esta muy bien
sobre todo si vas vestido para la ocasion



Capítulo 8

1. Palabra clave: loapa. Long: 7

   solo se tiene miedo cuando
   se esta en disensión consigo mismo

2. Palabra clave: pitufo. Long: 6

   solo el pensamiento vivido tiene valor

3. Palabra clave: igneo. Long: 9

   si la mujer no cede nunca
   el hombre cede siempre

4. Palabra clave: abulico. Long: 4

   los hombres son individualistas
   se alegran del mal del projimo y

tienden a separarse unos de otros y
solo se unen cuando se convencen de que
necesitan hacerlo si quieren reventar a un
enemigo superior origen de los ejercitos
los sindicatos las sociedades de futbol etcetera

5. Palabra clave: jopelines. Long: 5

cuando esperes a un amigo
no tomes los latidos de tu corazon
por el ruido de los cascos de su caballo

6. Matriz: 4,5,5,6

por cognoscible dicho sea de paso
no quiero decir aquello que puede ser conocido
por medio de la percepción de los sentidos o
que puede ser comprendido por la mente
sino mas bien que puede decirse que es conocido
o que posee un conocimiento o conocibilidad
o por lo menos algo que puedas mencionar a
un amigo

7. Matriz: 3,7,8,9

los hombres con valor y caracter
siempre les han resultado un poco siniestros
a la gente

8. Matriz: 5,2,6,9

si obraramos todos logicamente
haria tiempo que la raza humana
habria desaparecido del planeta

9. Matriz: 1,4,8,9

tengo entendido que las acciones de los huevos
estan en alza me anime por ultimo a decir
fingiendo la despreocupacion de un hombre
que fusiona sociedades en sus momentos libres

10. Matriz: 1,32,23,43

cuando descartes lanzo su entimema pienso
luego existo engendro la moderna filosofia de
abolengo esencialmente psicologico

11. Número clave: 5269

la conjuncion maxima de jupiter y saturno
se verifica cuando se juntan en signo de
trigono igneo despues de haber salido
del trigono acuo

12. Número clave: 123456789

la mujer y el libro que necesitamos
llegaran a nuestras manos sin buscarlos

13. Número clave: 131313

los ferrocarriles del amor funcionan
con horarios distintos y
no se cruzan a tiempo jamas

14. Número clave: 54321

los hombres con tal de tener dinero
traicionan mienten se envilecen asesinan
venden a un amigo a un camarada a un hermano

15. Número clave: 51369

en la profunda meditación existe la
posibilidad de anular el tiempo
de ver toda la vida pasada presente y futura
a la vez entonces todo es bueno perfecto

Capítulo 9

1. Modo: c. Número clave: 12345

   ningun hombre ha llegado a ser el mismo por
   completo sin embargo cada cual aspira a
   llegar los unos a ciegas los otros con
   mas luz cada cual como puede

2. Modo: c. Número clave: 32897

   un hombre que lleva dinero en la cartera
   no necesita saber de cada idioma
   mas que seis frases
   traigame huevos fritos
   traigame carne asada
   traigame pescado en salsa
   la amo a usted
   lleveme a un buen hotel
   se ha olvidado usted de ponerme el salero

3. Modo: c. Número clave: 43689

   nunca he creído en la existencia de esos
   amores que nacen de pronto en el instante
   en que nos abrochamos el gaban o en el
   momento en que el cobrador del tranvia se
   chupa el dedo para arrancar nuestro billete

4. Modo: c. Número de clave: 4327

   el hombre es el ser mas ingenuo de
   la creacion y donde la mujer pone calculo
   el no pone mas que simpleza

5. Modo: c. Número clave: 74

   la mujer criatura vulgar y egoista
   de singular belleza corporal
   a quien la boberia de los poetas liricos
   ha colocado una corona real
   que le viene ancha

Apéndices

Los datos originales para estos apéndices se han obtenido del estudio realizado para el libro de Enrique Fontanillo *Estudio lexicométrico del diario "El País"*. En él se recogen las frecuencias absolutas de aparición de todas las palabras publicadas a lo largo de una semana en dicho diario. Para este libro hemos seleccionado las palabras con una aparición superior a dos veces por diez mil, esto es, aproximadamente las quinientas palabras más frecuentes.

Los resultados obtenidos pueden ser considerados, en principio, poco representativos por el tipo de palabras que aparecen, típicas del argot periodístico (partido, paro, huelga, etc.), pero resulta correcta a la hora de realizar conteos de letras, digramas y las palabras cortas más frecuentes (artículos, preposiciones, etc.).

NOTA.—A efectos de proceso informático hemos sustituido la letra "ñ" por la "w". Por tanto, todos los datos que aparecen en los listados referidos a la "w", en realidad se refieren a la "ñ".

Apéndice 1

Frecuencia relativa de las letras en los textos en español

Las letras en un texto normal en español van apareciendo con unas características de frecuencia constantes. Se acostumbra a dividirlas en tres grupos, conocidos como grupos de frecuencia altos, medios y bajos, respectivamente.

		Letra	*Frecuencia absoluta*	*Frecuencia relativa (%)*
Frecuencias altas	1	E	88323	16.78
	2	A	62972	11.96
	3	O	45727	8.69
	4	L	44082	8.37
	5	S	41476	7.88
	6	N	36888	7.01
	7	D	36188	6.87
				68 %
Frecuencias medias	8	R	26016	4.94
	9	U	25303	4.80
	10	I	21836	4.15
	11	T	17438	3.31
	12	C	15407	2.92
	13	P	14532	2.76
	14	M	11187	2.12
				25 %

	Letra		Frecuencia absoluta	Frecuencia relativa (%)
Frecuencias bajas	15	Y	8122	1.54
	16	Q	8052	1.53
	17	B	4846	0.92
	18	H	4690	0.89
	19	G	3884	0.73
	20	F	2746	0.52
	21	V	2080	0.39
	22	W	1627	0.30
	23	J	1554	0.29
	24	Z	830	0.15
	25	X	353	0.06
	26	K	0	0.00
				7 %

Muestra = 526.159 letras

Las frecuencias relativas también se muestran en el histograma de la figura A1.

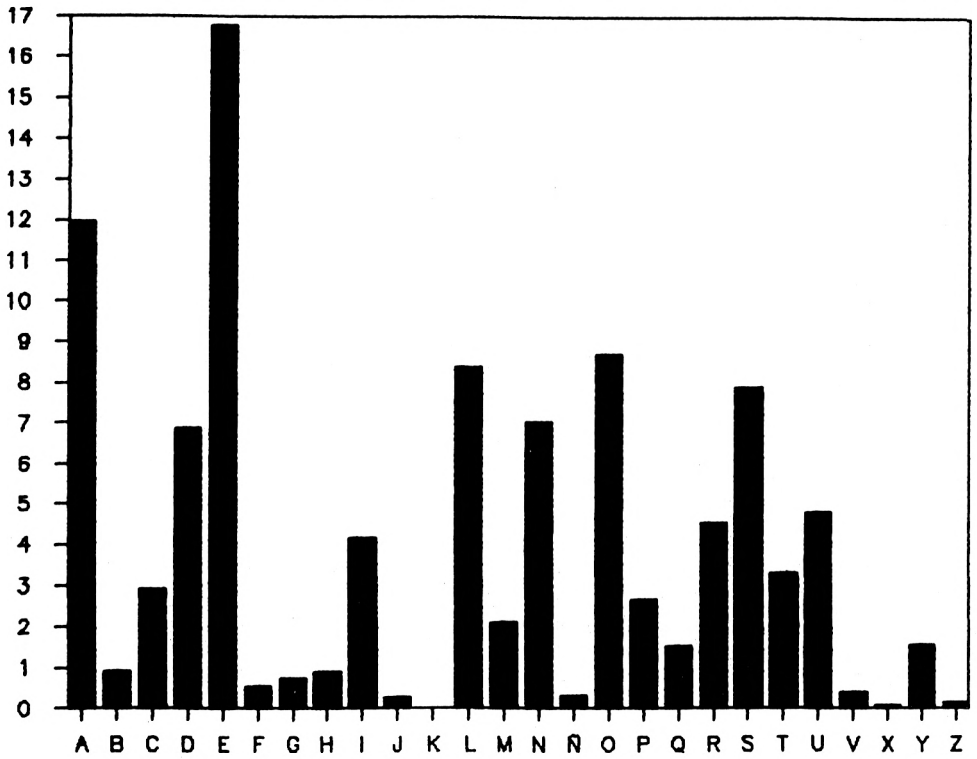


Figura A1

Los valores de esta tabla no se deberían tomar como exactos. Son el resultado de un muestreo estadístico y hay un cierto margen de error en todos los porcentajes individuales. Como una guía de ayuda para usar esta tabla de frecuencias se deberían tener en cuenta los siguientes comentarios.

Los datos de las frecuencias de las letras son siempre más fiables cuando se aplican a grupos de letras que a letras individuales. Por tanto, las siguientes reglas serían:

a) Las frecuencias relativas de las vocales y consonantes tienen recurrencias más importantes en los textos de cualquier longitud. En números redondos las vocales ocupan el 47 por 100 y las consonantes el 53 por 100.

b) Solamente dos letras se pueden identificar con seguridad sobre la base de las frecuencias individuales de las letras: E y A. Es aparente en el histograma de frecuencias que estas dos letras se destacan por sí mismas. Dado un texto de una longitud adecuada estas letras se pueden identificar simplemente sobre la base de las frecuencias de las letras:
   — El grupo de frecuencias alto ocupa algo más del 68 por 100 del texto, nuevamente con un buen grado de consistencia.
   — Las frecuencias relativas de las letras en los grupos alto, medio y bajo pueden variar, pero no suelen ser frecuentes los cambios de frecuencia para localizar una letra en un grupo distinto.
   — Las consonantes más frecuentes son L, S, N y D, ya que ocupan aproximadamente un 30 por 100 de los textos en español.
   — Las seis letras menos frecuentes son V, Ñ, J, Z, X y K, que ocupan algo más del 1 por 100 de los textos en español.

Siempre que se utilicen los datos de las frecuencias de las letras para resolver programas, se deben comprobar todas las suposiciones acerca de las letras individuales contrastándolas con las reglas de aquel grupo al cual pertenecen.

Apéndice 2

Frecuencias de digramas en los textos en español

Así como las letras individuales tienen sus propias frecuencias que las distinguen de las demás, ocurre lo mismo con los pares de letras, llamados "digramas". Muchos libros de criptografía incluyen datos de frecuencias de digramas. Lamentablemente, a pesar de ello, se necesita mucho más texto para conseguir una contabilización exacta de digramas que el necesario para las letras individuales. Existen marcadas diferencias entre los datos de los digramas publicados basados en muestreos de distintas magnitudes.

La tabla A2.1 da la frecuencia absoluta, para un muestreo de 526.159 digramas, de aparición de letras de la columna izquierda seguidas por letras de la fila superior. Asimismo, en la columna de la derecha se da el total de apariciones de cada letra como primera de un diagrama y, en la fila inferior, como segunda.

Tabla A2.1.—*Cuenta de digramas sobre una muestra de 526.159 digramas*

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	0	852	2157	2906	0	109	238	184	272	359	0	4237	710
B	934	0	0	0	501	0	0	0	1330	0	0	577	0
C	1626	0	178	0	1277	0	0	591	3442	0	0	324	0
D	1747	0	0	0	26769	0	0	0	1333	0	0	0	141
E	400	171	1881	724	106	264	922	0	78	205	0	13743	1540
F	78	0	0	0	558	0	0	0	328	0	0	99	0
G	672	0	0	0	315	0	0	0	84	0	0	0	0
H	2836	0	0	0	288	0	0	0	129	0	0	0	0
I	2412	375	1638	2303	2262	0	123	0	65	90	0	709	929
J	134	0	0	0	0	0	0	0	0	0	0	0	0
K	0	0	0	0	0	0	0	0	0	0	0	0	0
L	15510	0	0	0	1245	0	498	0	1492	0	0	742	56
M	3140	1005	0	0	1692	0	0	0	2174	0	0	0	0
N	3877	0	717	1150	1678	207	197	0	1688	51	0	0	0
O	0	1440	734	990	61	178	63	0	0	0	0	1513	1848
P	4515	0	0	0	1331	0	0	0	293	0	0	235	0
Q	0	0	0	0	0	0	0	0	0	0	0	0	0
R	5921	0	338	449	4822	0	349	0	2228	0	0	75	376
S	1282	0	153	355	6269	0	0	0	2960	0	0	0	259
T	4197	114	0	0	3791	0	0	0	1925	0	0	0	0
U	1017	372	385	154	10992	0	223	0	375	0	0	583	99
V	524	0	0	0	373	0	0	0	638	0	0	0	0
W	495	0	0	0	0	0	0	0	86	0	0	0	0
X	0	0	0	0	0	0	0	0	211	0	0	0	0
Y	442	0	0	0	748	0	0	0	0	0	0	0	0
Z	229	0	0	0	0	0	0	0	0	0	0	0	0
TOT	51988	4329	8181	9031	65078	758	2613	775	21131	705	0	22837	5958

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	TOT
A	3657	0	194	0	4498	7591	292	397	233	1575	0	1132	55	31648
B	0	165	0	0	1230	0	0	109	0	0	0	0	0	4846
C	84	5189	0	0	102	0	917	1488	0	0	0	0	0	15218
D	0	3961	0	0	598	0	0	347	0	0	0	0	0	34896
E	12179	71	198	103	5771	10315	495	207	557	52	198	125	356	50661
F	0	378	0	0	288	0	0	1017	0	0	0	0	0	2746
G	0	1221	0	0	487	0	63	1042	0	0	0	0	0	3884
H	0	1224	0	0	0	0	0	213	0	0	0	0	0	4690
I	2163	3669	277	0	488	1963	871	100	271	0	0	0	143	20851
J	0	799	0	0	0	0	0	631	0	0	0	0	0	1554
K	0	0	0	0	0	0	0	0	0	0	0	0	0	0
L	0	7067	0	89	0	0	447	451	0	0	0	0	0	27597
M	0	1597	792	0	0	0	0	693	0	0	0	0	0	11093
N	0	3640	0	192	0	453	4376	756	116	0	0	0	77	19175
O	7104	0	440	0	5341	8936	847	0	0	0	155	369	59	30078
P	52	4703	0	0	1977	61	114	1107	0	0	0	0	0	14388
Q	0	0	0	0	0	0	0	8052	0	0	0	0	0	8052
R	777	3025	0	156	181	251	1042	125	170	0	0	0	65	20350
S	0	2286	1179	0	0	0	4070	2446	0	0	0	0	0	21259
T	0	2945	0	0	3578	0	0	620	53	0	0	0	0	17223
U	7266	0	125	0	613	869	235	0	58	0	0	320	0	23686
V	0	388	0	0	0	0	0	52	0	0	0	0	0	1975
W	116	930	0	0	0	0	0	0	0	0	0	0	0	1627
X	0	0	0	0	0	0	142	0	0	0	0	0	0	353
Y	0	436	0	0	0	0	0	77	0	0	0	0	0	1703
Z	0	186	0	0	0	0	0	0	0	0	0	0	0	415
TOT	33399	43870	3205	540	25152	30439	13911	19930	1458	1627	353	1946	755	

La tabla A2.2 es una lista de las frecuencias de contacto por el lado izquierdo. Muestra para cada letra de la columna de la izquierda, en tantos por ciento, el número de veces que aparece precedida por la letra de la fila superior.

Tabla A2.2.—*Tabla de las frecuencias de contacto por el lado izquierdo*

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	0.00	2.95	5.13	5.52	1.26	0.24	2.12	8.96	7.62	0.42	0.00	49.00	9.92
B	17.58	0.00	0.00	0.00	3.52	0.00	0.00	0.00	7.73	0.00	0.00	0.00	20.73
C	14.17	0.00	1.16	0.00	12.36	0.00	0.00	0.00	10.76	0.00	0.00	0.00	0.00
D	8.32	0.00	0.00	0.00	2.07	0.00	0.00	0.00	6.59	0.00	0.00	0.00	0.00
E	0.00	0.98	2.52	52.83	0.20	1.10	0.62	0.56	4.46	0.00	0.00	2.45	3.33
F	3.96	0.00	0.00	0.00	9.61	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
G	6.12	0.00	0.00	0.00	23.73	0.00	0.00	0.00	3.16	0.00	0.00	12.82	0.00
H	3.92	0.00	12.60	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
I	1.30	6.37	16.50	6.39	0.37	1.57	0.40	0.61	0.31	0.00	0.00	7.15	10.42
J	23.10	0.00	0.00	0.00	13.19	0.00	0.00	0.00	5.79	0.00	0.00	0.00	0.00
K	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
L	15.35	2.09	1.17	0.00	49.79	0.35	0.00	0.00	2.56	0.00	0.00	2.68	0.00
M	6.40	0.00	0.00	1.27	13.88	0.00	0.00	0.00	8.37	0.00	0.00	0.50	0.00
N	19.07	0.00	0.43	0.00	63.51	0.00	0.00	0.00	11.28	0.00	0.00	0.00	0.00
O	0.00	0.54	17.25	13.16	0.23	1.25	4.05	4.06	12.19	2.62	0.00	23.49	5.30
P	1.34	0.00	0.00	0.00	1.37	0.00	0.00	0.00	1.92	0.00	0.00	0.00	5.50
Q	0.00	0.00	0.00	0.00	1.27	0.00	0.00	0.00	0.00	0.00	0.00	1.10	0.00
R	22.10	6.04	0.50	2.93	28.35	1.41	2.39	0.00	2.39	0.00	0.00	0.00	0.00
S	35.70	0.00	0.00	0.00	48.52	0.00	0.00	0.00	9.23	0.00	0.00	0.00	0.00
T	1.69	0.00	5.32	0.00	2.87	0.00	0.36	0.00	5.05	0.00	0.00	2.59	0.00
U	1.67	0.46	6.28	1.46	0.87	4.29	4.39	0.89	0.42	2.66	0.00	1.90	2.92
V	11.79	0.00	0.00	0.00	28.20	0.00	0.00	0.00	13.72	0.00	0.00	0.00	0.00
W	96.80	0.00	0.00	0.00	3.19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
X	0.00	0.00	0.00	0.00	56.09	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Y	66.47	0.00	0.00	0.00	7.33	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Z	13.25	0.00	0.00	0.00	85.78	0.00	0.00	0.00	34.45	0.00	0.00	0.00	0.00

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	12.25	0.00	14.26	0.00	18.70	4.05	13.26	3.21	1.65	1.56	0.00	1.39	0.72
B	0.00	29.71	0.00	0.00	0.00	0.00	2.35	7.67	0.00	0.00	0.00	0.00	0.00
C	4.71	4.82	0.00	0.00	2.22	1.00	0.00	2.52	0.00	0.00	0.00	0.00	0.00
D	3.29	2.83	0.00	0.00	1.28	1.01	0.00	0.44	0.00	0.00	0.00	0.00	0.00
E	3.31	0.12	2.62	0.00	9.51	12.37	7.48	21.69	0.73	0.00	0.00	1.47	0.00
F	7.53	6.48	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
G	5.07	1.62	0.00	0.00	8.98	0.00	0.00	5.74	0.00	0.00	0.00	0.00	0.00
H	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
I	8.09	0.00	1.40	0.00	10.68	14.19	9.23	1.79	3.05	0.41	1.01	0.00	0.00
J	3.28	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
K	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
L	0.00	5.48	0.85	0.00	0.27	0.00	0.00	2.11	0.00	0.00	0.00	0.00	0.00
M	0.00	16.65	0.00	0.00	3.38	2.33	0.00	0.89	0.00	0.00	0.00	0.00	0.00
N	0.00	37.04	0.27	0.00	4.03	0.00	0.00	37.89	0.00	0.60	0.00	0.00	0.00
O	12.10	0.00	15.63	0.00	10.05	7.60	9.79	0.00	1.28	3.09	0.00	1.44	0.61
P	0.00	3.05	0.00	0.00	0.00	8.19	0.00	0.86	0.00	0.00	0.00	0.00	0.00
Q	2.38	0.00	0.00	0.00	1.93	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
R	0.00	26.24	9.71	0.00	0.88	0.00	17.58	3.01	0.00	0.00	0.00	0.00	0.00
S	2.13	42.03	0.28	0.00	1.18	0.00	0.00	4.08	0.00	0.00	0.00	0.00	0.00
T	25.40	4.91	0.66	0.00	6.05	23.63	0.00	1.36	0.00	0.00	0.82	0.00	0.00
U	3.19	0.00	4.67	33.99	0.52	10.32	2.61	0.00	0.21	0.00	0.00	0.32	0.00
V	5.87	0.00	0.00	0.00	8.60	0.00	2.68	2.93	0.00	0.00	0.00	0.00	0.00
W	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
X	0.00	43.90	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Y	0.00	21.66	0.00	0.00	0.00	0.00	0.00	18.79	0.00	0.00	0.00	0.00	0.00
Z	18.55	14.21	0.00	0.00	15.66	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

La tabla A2.3 da las frecuencias de contacto por el lado derecho. Muestra para cada letra de la columna de la izquierda, en tanto por ciento, el número de veces que aparece seguida por la letra de la fila superior.

Tabla A2.3.—*Tabla de las frecuencias de contacto por el lado derecho*

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	0.00	2.69	6.81	9.18	0.00	0.34	0.75	0.58	0.85	1.13	0.00	13.38	2.24
B	19.27	0.00	0.00	0.00	10.33	0.00	0.00	0.00	27.44	0.00	0.00	11.90	0.00
C	10.68	0.00	1.16	0.00	8.39	0.00	0.00	3.88	22.61	0.00	0.00	2.12	0.00
D	5.00	0.00	0.00	0.00	76.71	0.00	0.00	0.00	3.81	0.00	0.00	0.00	0.40
E	0.78	0.33	3.71	1.42	0.20	0.52	1.81	0.00	0.15	0.40	0.00	27.12	3.03
F	2.84	0.00	0.00	0.00	20.32	0.00	0.00	0.00	11.94	0.00	0.00	3.60	0.00
G	17.30	0.00	0.00	0.00	8.11	0.00	0.00	0.00	2.16	0.00	0.00	0.00	0.00
H	60.46	0.00	0.00	0.00	6.14	0.00	0.00	0.00	2.75	0.00	0.00	0.00	0.00
I	11.56	1.79	7.85	11.04	10.94	0.00	0.58	0.00	0.31	0.43	0.00	3.40	4.45
J	8.62	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
K	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
L	56.20	0.00	0.00	0.00	4.51	0.00	1.80	0.00	5.40	0.00	0.00	2.68	0.20
M	28.30	9.05	0.00	0.00	15.25	0.00	0.00	0.00	19.59	0.00	0.00	0.00	0.00
N	20.21	0.00	3.73	5.99	8.75	1.07	1.02	0.00	8.80	0.26	0.00	0.00	0.00
O	0.00	4.78	2.44	3.29	0.20	0.59	0.20	0.00	0.00	0.00	0.00	5.03	6.14
P	31.38	0.00	0.00	0.00	9.25	0.00	0.00	0.00	2.03	0.00	0.00	1.63	0.00
Q	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
R	29.09	0.00	1.66	2.20	23.69	0.00	1.71	0.00	10.94	0.00	0.00	0.36	1.84
S	6.03	0.00	0.71	1.66	29.48	0.00	0.00	0.00	13.92	0.00	0.00	0.00	1.21
T	24.36	0.66	0.00	0.00	22.01	0.00	0.00	0.00	11.17	0.00	0.00	0.00	0.00
U	4.29	1.57	1.62	0.65	46.40	0.00	0.94	0.00	1.58	0.00	0.00	2.46	0.41
V	26.53	0.00	0.00	0.00	18.88	0.00	0.00	0.00	32.30	0.00	0.00	0.00	0.00
W	30.42	0.00	0.00	0.00	0.00	0.00	0.00	0.00	5.29	0.00	0.00	0.00	0.00
X	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	59.77	0.00	0.00	0.00	0.00
Y	25.95	0.00	0.00	0.00	43.92	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Z	55.18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	11.55	0.00	0.61	0.00	14.21	23.98	0.92	1.25	0.73	4.97	0.00	3.57	0.17
B	0.00	3.40	0.00	0.00	25.38	0.00	0.00	2.24	0.00	0.00	0.00	0.00	0.00
C	0.55	34.09	0.00	0.00	0.67	0.00	6.02	9.77	0.00	0.00	0.00	0.00	0.00
D	0.00	11.35	0.00	0.00	1.71	0.00	0.00	0.99	0.00	0.00	0.00	0.00	0.00
E	24.04	0.14	0.39	0.20	11.39	20.36	0.97	0.40	1.09	0.10	0.39	0.24	0.70
F	0.00	13.76	0.00	0.00	10.48	0.00	0.00	37.03	0.00	0.00	0.00	0.00	0.00
G	0.00	31.43	0.00	0.00	12.53	0.00	1.62	26.82	0.00	0.00	0.00	0.00	0.00
H	0.00	26.09	0.00	0.00	0.00	0.00	0.00	4.54	0.00	0.00	0.00	0.00	0.00
I	10.37	17.59	1.32	0.00	2.54	9.41	4.17	0.47	1.29	0.00	0.00	0.00	0.68
J	0.00	50.77	0.00	0.00	0.00	0.00	0.00	40.60	0.00	0.00	0.00	0.00	0.00
K	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
L	0.00	25.60	0.00	0.32	0.00	0.00	1.61	1.63	0.00	0.00	0.00	0.00	0.00
M	0.00	14.39	7.13	0.00	0.00	0.00	0.00	6.24	0.00	0.00	0.00	0.00	0.00
N	0.00	18.98	0.00	1.00	0.00	2.36	22.82	3.94	0.60	0.00	0.00	0.00	0.40
O	23.61	0.00	1.46	0.00	17.75	29.70	2.81	0.00	0.00	0.00	0.51	1.22	0.19
P	0.36	32.69	0.00	0.00	13.74	0.42	0.79	7.69	0.00	0.00	0.00	0.00	0.00
Q	0.00	0.00	0.00	0.00	0.00	0.00	0.00	100.00	0.00	0.00	0.00	0.00	0.00
R	3.81	14.86	0.00	0.76	0.88	1.23	5.12	0.61	0.83	0.00	0.00	0.00	0.31
S	0.00	10.75	5.54	0.00	0.00	0.00	19.14	11.50	0.00	0.00	0.00	0.00	0.00
T	0.00	17.09	0.00	0.00	20.77	0.00	0.00	3.59	0.30	0.00	0.00	0.00	0.00
U	30.67	0.00	0.52	0.00	2.58	3.66	0.99	0.00	0.24	0.00	0.00	1.35	0.00
V	0.00	19.64	0.00	0.00	0.00	0.00	0.00	2.63	0.00	0.00	0.00	0.00	0.00
W	7.12	57.16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
X	0.00	0.00	0.00	0.00	0.00	0.00	40.22	0.00	0.00	0.00	0.00	0.00	0.00
Y	0.00	25.60	0.00	0.00	0.00	0.00	0.00	4.52	0.00	0.00	0.00	0.00	0.00
Z	0.00	44.81	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Como con las frecuencias de las letras individuales, también existen ciertas reglas adicionales que se deben tener en cuenta para utilizar mejor los datos de los digramas.

1. La mayor parte de los textos cifrados serán considerablemente más cortos que el muestreo en el cual se basa la cuenta de los digramas. Se necesita mucho más cuidado cuando se utilizan los datos de los digramas que las frecuencias de las letras individuales.
2. Si se utilizan los datos de los digramas para identificar el texto original de las letras del texto del cifrado, se deberán comprobar todas las suposiciones de equivalencia con las reglas dadas para las frecuencias de las letras individuales.
3. Una buena forma de utilizar los datos de los digramas para obtener los textos originales de los cifrados es aprovechar los datos de los contactos para identificar a las letras vecinas antes que hacerlo con las reglas para las frecuencias de las letras individuales.
4. El examen de los datos de las frecuencias de los digramas mostrará qué pares de letras inversas son comunes (por ejemplo, ER y RE pueden aparecer más frecuentemente que otros pares). A veces resulta útil para la identificación de un par de letras la relación existente entre la frecuencia de aparición del digrama y la frecuencia de aparición de su inversa. La tabla A2.4 muestra los datos de las relaciones para los pares inversos más comunes.
5. También ciertos grupos se pueden identificar entre los digramas más comunes, como se muestra en la tabla A2.4.
6. Sólo algunos digramas dobles (dos letras iguales) son comunes (véase la miscelánea de datos).

La mayor parte de los análisis criptológicos de este libro utilizan las frecuencias de las letras y las frecuencias de contacto por el lado derecho dados en este apéndice. Por tanto, estos datos deben estar de forma que sean legibles por el ordenador. El siguiente programa creará una tabla relativa a las frecuencias de las letras individuales y otra de las frecuencias de contacto por el lado derecho grabados con forma de ficheros en una cinta. Los datos que se deben introducir están contenidos en la primera tabla de este apéndice y en la tabla A2.3.

```
10 REM PROGRAMA DE CREACION
          DE DATOS
11 RANDOMIZE 3
15 PRINT "PROGRAMA DE CREACION
DE DATOS"
20 PRINT AT 2,0;"ESCRIBA LA FR
ECUENCIA PARA CADA LETRA SEGUN S
E PIDA"
30 DIM e(26)
40 FOR i=1 TO 26
```

```
  50 LET e(i)=RND
  60 NEXT i
  70 PRINT AT 4,0;"ESCRIBA AHORA
 LOS DATOS DE TRANSICION PARA CA
DA PAR DE LETRAS"
  80 DIM t(26,26)
  90 FOR i=1 TO 26
 100 FOR j=1 TO 26
 110  LET t(i,j)=RND
 120 NEXT j
 130 NEXT i
 140 PRINT AT 6,0;"INTRODUZCA LA
 CINTA PARA ALMACENAR LOS DATOS
,Y PULSE LUEGO CUALQUIER TECLA."
 150 PAUSE 0
 160 SAVE *"m";2;"frecuencia" DA
TA e()
 170 SAVE *"m";2;"transicion" DA
TA t()
```

Anotaciones del programa de almacenamiento de datos

Líneas	
10-30	Inicialización.
40-60	Introducción de las frecuencias de las letras individuales.
70-130	Introducción de los datos relativos a los contactos.
140-170	Archivo en cinta.

Tabla A2.4.—*Digramas más comunes*

	DIGRAMA	FRECUENCIA	INVERSA	RELACION
1	DE	26769	724	36.97
2	LA	15510	4237	3.66
3	EL	13743	1245	11.04
4	EN	12169	1678	7.26
5	UE	10992	207	53.10
6	ES	10315	6269	1.65
7	OS	8936	2286	3.91
8	QU	8052	0	****
9	UN	7266	756	9.61
10	ON	7104	3640	1.95
11	RA	5921	4498	1.32
12	AS	5791	1282	5.92
13	ER	5771	4822	1.20
14	OR	5341	3025	1.77
15	CO	5189	734	7.07

Digramas más comunes

DE, LA Grupo de frecuencias altas.
EN, UE, ES Grupo de frecuencias medias.

Utilice esta tabla con extrema precaución. No la utilice como una base sólida para identificar letras, sino como una sugerencia solamente.

Miscelánea de datos

Los digramas de letras dobles más comunes son, en orden de frecuencia: LL, RR, CC.

Apéndice 3

Frecuencias de palabras y otros datos varios

Cuando se conocen los límites de las palabras dentro de un criptograma (e incluso si no se conocen), se pueden utilizar los datos sobre la frecuencia de palabras para identificarlas o incluso hasta grupos de ellas.

Este apéndice contiene los datos que pueden resultar más útiles sobre frecuencias de palabras. Todas estas tablas están realizadas a partir del estudio citado al comienzo de estos apéndices realizados sobre una semana de publicaciones del diario *El País*, por lo que incluyen palabras y siglas características de un periódico.

La tabla A3.1 contiene las palabras con una frecuencia de aparición superior a dos apariciones por diez mil.

Las tablas A3.2 a A3.5 tienen la lista de palabras de dos, tres, cuatro y cinco letras más frecuentes.

La tabla A3.6 contiene la lista de frecuencias de las letras individuales como iniciales y finales de palabra.

Tabla A3.1.—*Palabras con una frecuencia de aparición superior a dos por diez mil*

Término	*Frec. abs.*	*Frec. rel.* ‰	*Término*	*Frec. abs.*	*Frec. rel.* ‰	*Término*	*Frec. abs.*	*Frec. rel.* ‰
DE	19711	778.1	CUANDO	247	9.7	ALGUNOS	138	5.4
LA	11646	459.7	A%O	235	9.2	NUEVO	137	5.4
EL	8581	338.7	ANTE	230	9	NUEVA	137	5.4
EN	7640	301.6	DURANTE	229	9	ERA	137	5.4
QUE	7315	288.7	MINISTRO	221	8.7	TIEMPO	136	5.3
Y	5726	226	HABIA	220	8.6	TANTO	136	5.3
A	5394	212.9	HUELGA	213	8.4	CONSEJO	136	5.3
LOS	4960	195.8	ESTADO	210	8.2	SINO	135	5.3
DEL	3957	156.2	BARCELONA	208	8.2	TRABAJADORES	134	5.2
SE	3019	119.1	PUEDE	205	8	PRIMER	131	5.1
LAS	2890	114	HOY	205	8	JUAN	131	5.1
POR	2796	110.3	TIENE	201	7.9	D	131	5.1
UN	2483	98	TRES	200	7.8	VIDA	129	5
CON	2092	82.5	DIA	200	7.8	FUERON	129	5
UNA	1977	78	AUNQUE	192	7.5	ANTES	128	5
NO	1873	73.9	JOSE	190	7.5	SOCIAL	127	5
PARA	1698	67	ESPA%OL	190	7.5	PARECE	127	5
SU	1617	63.8	OTROS	187	7.3	MINISTERIO	127	5
AL	1591	62.8	HACE	187	7.3	FORMA	127	5
ES	1184	46.7	E	187	7.3	ESTAN	127	5
HA	1064	42	TODOS	185	7.3	REUNION	125	4.9
COMO	909	35.8	ESTOS	185	7.3	PUBLICO	125	4.9
MAS	903	35.6	DONDE	184	7.2	LEY	125	4.9
LO	795	31.3	AHORA	184	7.2	GRUPO	125	4.9
SOBRE	684	27	PRIMERA	183	7.2	CADA	124	4.8
SUS	682	26.9	HAY	183	7.2	EMPRESA	123	4.8
AYER	642	25.3	POLITICA	181	7.1	CUATRO	123	4.8
ESTE	596	23.5	MUY	180	7.1	DIRECCION	122	4.8
O	584	23	MISMO	180	7.1	COMUNIDAD	121	4.7
ENTRE	557	21.9	HORAS	175	6.9	PERSONAS	120	4.7
MADRID	531	20.9	CASO	174	6.8	MUNDO	118	4.6
HAN	484	19.1	ASI	173	6.8	DEBE	118	4.6
PERO	469	18.5	PAIS	169	6.6	LES	117	4.6
GOBIERNO	468	18.4	DIAS	167	6.5	FIN	116	4.5
DOS	466	18.3	UNOS	166	6.5	ESPA%NOLES	116	4.5
SEGUN	450	17.7	TRABAJO	166	6.5	UNAS	115	4.5
SIN	432	17	PARTIDO	166	6.5	TAN	115	4.5
ESTA	432	17	TRAS	164	6.4	FRENTE	115	4.5
FUE	421	16.6	UNO	159	6.2	ACTUAL	115	4.5
YA	369	14.5	ESTAS	158	6.2	SEPTIEMBRE	114	4.5
PARTE	365	14.4	PORQUE	156	6.1	HABER	113	4.4
MILLONES	364	14.3	OTRA	155	6.1	C	113	4.4
DESDE	355	14	FUENTES	154	6	SERA	112	4.4
A%OS	353	13.9	DIRECTOR	154	6	HACER	112	4.4
ESPA%A	344	13.5	HECHO	153	6	COMISION	111	4.3
GENERAL	315	12.4	ESPA%OLA	152	6	POCO	110	4.3
TAMBIEN	310	12.2	DESPUES	152	6	OTRAS	110	4.3
PRESIDENTE	308	12.1	NI	150	5.9	OTAN	109	4.3
HASTA	308	12.1	EMBARGO	150	5.9	BIEN	109	4.3
SI	300	11.8	MENOS	149	5.8	ESTADOS	108	4.2
LE	293	11.5	NACIONAL	148	5.8	SISTEMA	107	4.2
PASADO	292	11.5	GRAN	147	5.8	QUIEN	106	4.1
SER	286	11.2	OTRO	145	5.7	PROYECTO	106	4.1
TODO	282	11.1	P	144	5.6	ESA	106	4.1
PESETAS	273	10.7	DEFENSA	143	5.6	CEE	106	4.1
SON	269	10.6	VEZ	141	5.5	NOS	105	4.1
SIDO	269	10.6	MAYOR	141	5.5	MIEMBROS	105	4.1
ACUERDO	255	10	ADMINISTRACION	141	5.5	CENTRO	105	4.1
SOLO	251	9.9	SITUACION	140	5.5	PROXIMO	104	4.1
CONTRA	250	9.8	MOMENTO	138	5.4	IBERIA	104	4.1
ESTA	249	9.8	ME	138	5.4	S	104	4.1

Término	*Frec. abs.*	*Frec. rel. °/ooo*
SEGURIDAD	103	4
SECTOR	103	4
PAISES	103	4
EQUIPO	103	4
ELLOS	103	4
SENTIDO	102	4
SECRETARIO	102	4
MES	102	4
SEMANA	101	3.9
SIEMPRE	100	3.9
CIUDAD	100	3.9
REAL	99	3.9
NUMERO	99	3.9
MA%ANA	99	3.9
DECISION	99	3.9
COFLICTO	99	3.9
SEA	98	3.8
MESES	98	3.8
CUENTA	98	3.8
COMITE	98	3.8
UNIDOS	96	3.7
TODA	96	3.7
SEGUNDA	96	3.7
POLICIA	96	3.7
CLUBES	96	3.7
RESPECTO	95	3.7
POSIBLE	95	3.7
VASCO	94	3.7
MEDIO	94	3.7
M	94	3.7
ADEMAS	94	3.7
ULTIMOS	93	3.6
ASUNTOS	93	3.6
SAN	92	3.6
PUBLICA	92	3.6
PODER	92	3.6
MILITAR	92	3.6
MIENTRAS	92	3.6
CINCO	92	3.6
QUE	91	3.5
EXTERIORES	91	3.5
EMPRESAS	91	3.5
ELLO	91	3.5
EL	91	3.5
TODAS	90	3.5
SERVICIO	90	3.5
PUNTO	90	3.5
DIJO	90	3.5
AUN	90	3.5
TIENEN	89	3.5
REAGAN	89	3.5
MAYORIA	89	3.5
CUALQUIER	89	3.5
CASI	89	3.5
R	88	3.4
LUGAR	88	3.4
HABIAN	88	3.4
FRANCES	88	3.4
ORGANIZACION	87	3.4
JULIO	87	3.4
TEMA	86	3.3
SOCIALISTA	86	3.3
INTERNACIONAL	86	3.3
COMPA%IA	86	3.3
BASE	86	3.3
ULTIMA	85	3.3
FRANCIA	85	3.3
FERNANDEZ	85	3.3
TELEVISION	84	3.3
TECNICOS	84	3.3
T	84	3.3
REPRESENTANTES	84	3.3
PAGINA	84	3.3
NADA	84	3.3
MUCHOS	84	3.3
DENTRO	84	3.3
PRESA	83	3.2
MARIA	83	3.2
FESTIVAL	83	3.2
CAMBIO	83	3.2
TARDE	82	3.2
TAL	82	3.2
PARTIR	82	3.2
EUROPA	82	3.2
YO	81	3.1
NOCHE	81	3.1
VA	80	3.1
SERVICIO	80	3.1
MANUEL	80	3.1
MANTENIMIENTO	80	3.1
ESTABA	80	3.1
ALGO	80	3.1
OFICIAL	79	3.1
NEGOCIACIONES	79	3.1
MISMAS	79	3.1
MI	79	3.1
JORNADA	79	3.1
HORA	79	3.1
FALTA	78	3
SEIS	78	3
PROPIO	78	3
OPINION	78	3
INFORMACION	78	3
FINAL	78	3
PROBLEMA	77	3
MEDIDA	77	3
LUIS	77	3
HACIA	77	3
GONZALEZ	77	3
AYUNTAMIENTO	77	3
PROBLEMA	76	3
MEDIOS	76	3
GRANDES	76	3
CULTURA	76	3
CONGRESO	76	3
C	76	3
ZONA	75	2.9
UNION	75	2.9
PRIMEROS	75	2.9
ECONOMICAS	75	2.9
DECIR	75	2.9
CARLOS	75	2.9
CARACTER	75	2.9
SOCIEDAD	74	2.9
SI	74	2.9
PRESENCIA	74	2.9
MUCHO	74	2.9
TOTAL	73	2.8
PUNTOS	73	2.8
OBRAS	73	2.8
MERCADO	73	2.8
HISTORIA	73	2.8
CUYA	73	2.8
JUGADORES	72	2.8
INCLUSO	72	2.8
FUERA	73	2.8
ANTONIO	72	2.8
MEDIDAS	71	2.8
HOMBRES	71	2.8
EMPLEO	71	2.8
DERECHO	71	2.8
POPULAR	71	2.8
LIBERTAD	70	2.7
TIPO	69	2.7
RELACIONES	69	2.7
PERSONAL	69	2.7
MEJOR	69	2.7
ESTO	69	2.7
CIVIL	69	2.7
CAPITAL	69	2.7
ANTERIOR	69	2.7
TENER	68	2.6
POLITICO	68	2.6
PIVOT	68	2.6
OPOSICION	68	2.6
MINISTRO	68	2.6
ENTONCES	68	2.6
EFE	68	2.6
SEVILLA	67	2.6
PODRIA	67	2.6
PAPA	67	2.6
NEGOCIACION	67	2.6
DOLARES	67	2.6
CUYO	67	2.6
CAMPO	67	2.6
ALGUNAS	67	2.6
SEGUNDO	66	2.6
NUEVOS	66	2.6
NUEVAS	66	2.6
IMPORTANTE	66	2.6
CONFERENCIA	66	2.6
TRANSPORTE	65	2.5
PUEDEN	65	2.5
PERIODO	65	2.5
MILITARES	65	2.5
II	65	2.5
FUERZAS	65	2.5
ESPECIAL	65	2.5
DADO	65	2.5
AGOSTO	65	2.5
VARIOS	64	2.5
LUNES	64	2.5
INVESTIGACION	64	2.5
DICHO	64	2.5
DERECHOS	64	2.5
UGT	63	2.4
PROPUESTA	63	2.4
PROGRAMA	63	2.4
PESAR	63	2.4
MUERTE	63	2.4
INFORME	63	2.4
GUERRA	63	2.4
FUTBOL	63	2.4
DESARROLLO	63	2.4
VECES	62	2.4

Término	*Frec. abs.*	*Frec. rel.* ‰
PUES	62	2.4
OBRAS	62	2.4
NOMBRES	62	2.4
JUNTA	62	2.4
EDUCACION	62	2.4
DOMINGO	62	2.4
CURSO	62	2.4
AVIONES	62	2.4
ULTIMO	61	2.4
SIETE	61	2.4
PSOE	61	2.4
PARO	61	2.4
ORDEN	61	2.4
LARGO	61	2.4
JUEGO	61	2.4
FUTURO	61	2.4
ENCUENTRO	61	2.4
CUAL	61	2.4
CASA	61	2.4
TRATA	60	2.3
JUSTICIA	60	2.3
AUTORIDADES	60	2.3
PORTAVOZ	59	2.3
OCTUBRE	59	2.3
NINGUN	59	2.3
LIGA	59	2.3
FERNANDO	59	2.3
ESCOLAR	59	2.3
CUETION	59	2.3
CONDICIONES	59	2.3
BAJO	59	2.3
ASAMBLEA	59	2.3
TUVO	58	2.2
NUESTRO	58	2.2
ECONOMIA	58	2.2
APOYO	58	2.2
TODAVIA	57	2.2
TEMAS	57	2.2
NUESTRA	57	2.2
FONDO	57	2.2
ESTAR	57	2.2
CONTRATO	57	2.2
COMO	57	2.2
CERCA	57	2.2
PUESTO	56	2.2
PRODUCCION	56	2.2
PELICULA	56	2.2
NUNCA	56	2.2
HIZO	56	2.2
EXISTE	56	2.2
PESO	56	2.2
ACTUALMENTE	56	2.2
TRAVES	55	2.1
SECTORES	55	2.1
REALIDAD	55	2.1
PLENO	55	2.1
PLAZO	55	2.1
NECESIDAD	55	2.1
INSTITUCIONES	55	2.1
ENCUENTRA	55	2.1
DALI	55	2.1
CUANTO	55	2.1
CAUSA	55	2.1
CARRERA	55	2.1
BUENA	55	2.1
AFIRMO	55	2.1
TRIBUNAL	54	2.1
SOLUCION	54	2.1
RESULTADOS	54	2.1
PLAN	54	2.1
PARTIDOS	54	2.1
JUDICIAL	54	2.1
HE	54	2.1
ELLAS	54	2.1
CONSIDERA	54	2.1
AFE	54	2.1
TV	53	2
RELACION	53	2
REFORMA	53	2
PUEBLO	53	2
PARIS	53	2
MUNICIPAL	53	2
JUEZ	53	2
DIARIO	53	2
DECLARO	53	2
VUELOS	52	2
TEMPORADA	52	2
SINDICATO	52	2
SE%ALO	52	2
POSIBILIDAD	52	2
PNV	52	2
PARTICIPACION	52	2
ITALIA	52	2
ENTRADA	52	2
DECLARACIONES	52	2
SIENDO	51	2
SESION	51	2
SABADO	51	2
PROXIMA	51	2
PROCESO	51	2
POLITICOS	51	2
NIVEL	51	2
FUTBOLISTAS	51	2
EXTERIOR	51	2
DECLARACION	51	2
CONTROL	51	2
CONJUNTO	51	2
CENTRAL	51	2
CARGO	51	2
AMBOS	51	2
ACUERDOS	51	2

Tabla A3.2.—*Palabras de dos letras más frecuentes*

Térm.	*Frec. abs.*	*Frec. rel.*	*Térm.*	*Frec. abs.*	*Frec. rel.*
DE	19711	778.1	LO	795	31.3
LA	11646	459.7	YA	369	14.5
EL	8581	338.7	SI	300	11.8
EN	7640	301.6	LE	293	11.5
SE	3019	119.1	NI	150	5.9
UN	2483	98	ME	138	5.4
NO	1873	73.9	EL	91	3.5
SU	1617	63.8	YO	81	3.1
AL	1591	62.8	VA	80	3.1
ES	1184	46.7	MI	79	3.1
HA	1064	42	SI	74	2.9

Tabla A3.3.—*Palabras de tres letras más frecuentes*

Térm.	*Frec. abs.*	*Frec. rel.*	*Térm.*	*Frec. abs.*	*Frec. rel.*
QUE	7315	288.7	HAY	183	7.2
LOS	4960	195.8	MUY	180	7.1
DEL	3957	156.2	ASI	173	6.8
LAS	2890	114	UNO	159	6.2
POR	2796	110.3	VEZ	141	5.5
CON	2092	82.5	ERA	137	5.4
UNA	1977	78	LEY	125	4.9
MAS	903	35.6	LES	117	4.6
SUS	682	26.9	FIN	116	4.5
HAN	484	19.1	TAN	115	4.5
DOS	466	18.3	ESA	106	4.1
SIN	432	17	NOS	105	4.1
FUE	421	16.6	MES	102	4
SER	286	11.2	SEA	98	3.8
SON	269	10.6	SAN	92	3.6
A%O	235	9.2	QUE	91	3.5
HOY	205	8	AUN	90	3.5
DIA	200	7.8	TAL	82	3.2

Tabla A3.4.—*Palabras de cuatro letras más frecuentes*

Térm.	*Frec. abs.*	*Frec. rel.*	*Térm.*	*Frec. abs.*	*Frec. rel.*
PARA	1698	67	REAL	99	3.9
COMO	909	35.8	TODA	96	3.7
AYER	642	25.3	ELLO	91	3.5
ESTE	596	23.5	DIJO	90	3.5
PERO	469	18.5	CASI	89	3.5
ESTA	432	17	TEMA	86	3.3
A%OS	353	13.9	BASE	86	3.3
TODO	282	11.1	NADA	84	3.3
SIDO	269	10.6	ALGO	80	3.1
SOLO	251	9.9	HORA	79	3.1
ESTA	249	9.8	SEIS	78	3
ANTE	230	9	LUIS	77	3
TRES	200	7.8	ZONA	75	2.9
JOSE	190	7.5	CUYA	73	2.8
HACE	187	7.3	TIPO	69	2.7
CASO	174	6.8	ESTO	69	2.7
PAIS	169	6.6	PAPA	67	2.6
DIAS	167	6.5	CUYO	67	2.6
UNOS	166	6.5	DADO	65	2.5
TRAS	164	6.4	PUES	62	2.4
OTRA	155	6.1	PSOE	61	2.4
GRAN	147	5.8	PARO	61	2.4
OTRO	145	5.7	CUAL	61	2.4
SINO	135	5.3	CASA	61	2.4
JUAN	131	5.1	LIGA	59	2.3
VIDA	129	5	BAJO	59	2.3
CADA	124	4.8	TUVO	58	2.2
DEBE	118	4.6	COMO	57	2.2
UNAS	115	4.5	HIZO	56	2.2
SERA	112	4.4	PESO	56	2.2
POCO	110	4.3	DALI	55	2.1
OTAN	109	4.3	PLAN	54	2.1
BIEN	109	4.3	JUEZ	53	2

Tabla A3.5.—*Palabras de cinco letras más frecuentes*

Térm.	*Frec. abs.*	*Frec. rel.*
SOBRE	684	27
ENTRE	557	21.9
SEGUN	450	17.7
PARTE	365	14.4
DESDE	355	14
HASTA	308	12.1
HABIA	220	8.6
PUEDE	205	8
TIENE	201	7.9
OTROS	187	7.3
TODOS	185	7.3
ESTOS	185	7.3
DONDE	184	7.2
AHORA	184	7.2
MISMO	180	7.1
HORAS	175	6.9
ESTAS	158	6.2
HECHO	153	6
MENOS	149	5.8
MAYOR	141	5.5
NUEVO	137	5.4
NUEVA	137	5.4
TANTO	136	5.3
ANTES	128	5
FORMA	127	5
ESTAN	127	5
GRUPO	125	4.9
MUNDO	118	4.6
HABER	113	4.4
HACER	112	4.4
OTRAS	110	4.3
QUIEN	106	4.1
ELLOS	103	4
MESES	98	3.8
VASCO	94	3.7
MEDIO	94	3.7
PODER	92	3.6
CINCO	92	3.6
TODAS	90	3.5
PUNTO	90	3.5
LUGAR	88	3.4
JULIO	87	3.4
PRESA	83	3.2
MARIA	83	3.2

Térm.	*Frec. abs.*	*Frec. rel.*
TARDE	82	3.2
NOCHE	81	3.1
FALTA	78	3
FINAL	78	3
HACIA	77	3
UNION	75	2.9
DECIR	75	2.9
MUCHO	74	2.9
TOTAL	73	2.8
OBRAS	73	2.8
FUERA	73	2.8
MEJOR	69	2.7
CIVIL	69	2.7
TENER	68	2.6
PIVOT	68	2.6
CAMPO	67	2.6
LUNES	64	2.5
DICHO	64	2.5
PESAR	63	2.4
VECES	62	2.4
OBRAS	62	2.4
JUNTA	62	2.4
CURSO	62	2.4
SIETE	61	2.4
ORDEN	61	2.4
LARGO	61	2.4
JUEGO	61	2.4
TRATA	60	2.3
APOYO	58	2.2
TEMAS	57	2.2
FONDO	57	2.2
ESTAR	57	2.2
CERCA	57	2.2
NUNCA	56	2.2
PLENO	55	2.1
PLAZO	55	2.1
CAUSA	55	2.1
BUENA	55	2.1
ELLAS	54	2.1
PARIS	53	2
NIVEL	51	2
CARGO	51	2
AMBOS	51	2

Tabla A3.6.—*Frecuencia de las letras individuales como iniciales y finales de palabra*

LETRA	PRINCIPIO	FINAL
A	7.0	20.0
B	.3	.0
C	4.6	.1
D	17.3	.8
E	14.8	24.1
F	1.2	.0
G	.8	.0
H	2.5	.0
I	.4	.6
J	.5	.0
K	.0	.0
L	13.6	10.5
M	3.3	.0
N	2.2	11.3
O	1.1	10.0
P	7.2	.0
Q	4.8	.0
R	.5	3.6
S	7.0	12.9
T	2.2	.1
U	3.4	1.0
V	.3	.0
W	.0	.0
X	.0	.0
Y	3.9	4.1
Z	.0	.2

MUESTRA=156191 PALABRAS

Apéndice 4

Versiones de los programas para distintas máquinas

Programas para MSX

CESAR

```
1 REM *********
2 REM *       *
3 REM * CESAR *
4 REM *       *
5 REM *********
6 REM
10 SCREEN 0:KEY OFF:POKE -853,255:OUT
 170,255
20 PRINT TAB(5);"PROGRAMA DE CIFRADO
<CESAR>"
30 LOCATE 2,4
40 PRINT "MODO Y CLAVE: ";
50 INPUT M$
60 IF LEFT$(M$,1)="0" THEN GOTO 9999
70 IF LEFT$(M$,1)<"C" OR LEFT$(M$,1)>
"D" THEN GOTO 100
80 IF RIGHT$(M$,1)<"A" OR RIGHT$(M$,1
)>"Z" THEN GOTO 100
90 GOTO 120
100 LOCATE 15,4:PRINT SPC(10);:LOCATE
 15,4
110 GOTO 50
120  LOCATE 2,2:PRINT "MODO: ";LEFT$(
M$,1):PRINT TAB(2);"CLAVE: ";RIGHT$(M
$,1)
130 K=ASC(RIGHT$(M$,1))-ASC("A")
140 LOCATE 2,4:PRINT "TEXTO: ";SPC(15
):LOCATE 8,4
150 INPUT T$
160 IF LEFT$(T$,1)="0" THEN GOTO 9999
170 IF LEFT$(M$,1)="C" THEN GOTO 190
180 K=-K
190 L=LEN(T$)
195 LOCATE 2,9
200 FOR I=1 TO L
210 C$=MID$(T$,I,1)
220 IF C$>="A" AND C$<="Z" THEN GOTO
250
230 PRINT " ";
240 GOTO 280
250 W=ASC(C$)-ASC("A")+K
260 GOSUB 420
270 PRINT CHR$(W+ASC("A"));
280 NEXT I
```

```
290 IF LEFT$(M$,1)="C" THEN GOTO 9999
300  '
310 LOCATE 8,20: PRINT "PULSE <S> PAR
A SEGUIR":PRINT TAB(8);"O <N> PARA DE
TENERSE"
320 R$=INKEY$
330 IF R$="" THEN GOTO 320
340 IF R$="N" THEN GOTO 9999
350 IF R$="S" THEN GOTO 380
360 LOCATE 21,0:PRINT "? ";
370 GOTO 310
380 W=1-K
390 GOSUB 420
400 K=-W
410 GOTO 195
420 IF W<=25 THEN GOTO 440
430 W=W-26
440 IF W>=0 THEN GOTO 460
450 W=W+26
460 RETURN
9999 END
```

MONO

```
1 REM ************************
2 REM *                      *
3 REM * CIFRADO MONOALFABETICO *
4 REM *                      *
5 REM ************************
6 REM
10 KEYOFF:POKE -853,255:OUT 170,255:C
LEAR 1000:CLS
20 PRINT  TAB(1);"PROGRAMA DE CIFRADO
 MONOALFABETICO"
25 PRINT TAB(1);STRING$(34,61)
30 LOCATE 2,4
40 PRINT "MODO, MEZCLA Y CLAVE: ";
50 INPUT M$
60 IF M$="0" THEN GOTO 9999
70 L=LEN(M$)
80 IF L<3 OR L>28 THEN GOTO 150
90 IF LEFT$(M$,1)<"C" OR LEFT$(M$,1)>
"D" THEN GOTO 150
100 IF MID$(M$,2,1)<"S" OR MID$(M$,2,
1)>"T" THEN GOTO 150
110 FOR I=3 TO L
120 IF MID$(M$,I,1)<"A" OR MID$(M$,I,
1)>"Z" THEN GOTO 150
130 NEXT I
132 LOCATE 0,4:PRINT SPC(255):LOCATE
2,4:PRINT "MODO: ";MID$(M$,1,1);
134 LOCATE 2,5:PRINT "MEZCLA: ";MID$(
M$,2,1)
136 LOCATE 2,6:PRINT "CLAVE: ";MID$(M
$,3)
140 GOTO 220
150 LOCATE 9,15:PRINT "ENTRADA INVALI
DA":FOR T=1 TO 500:NEXT T:LOCATE 9,15
:PRINT SPC(40)
160 IF L>28 GOTO 190
170 LOCATE 23,4:PRINT SPC(255)
180 GOTO 200
190 LOCATE 25,4:PRINT MID$(M$,1,26);S
PC(255)
200 REM
210 GOTO 30
220 M$=M$+"ABCDEFGHIJKLMNOPQRSTUVWXYZ
"
230 LA=LEN(M$)
240 C$=""
250 CA=ASC("A")-1
260 A$=SPACE$(26)
270 FOR I=3 TO LA
280 AS=ASC(MID$(M$,I,1))-CA
290 IF MID$(A$,AS,1)<>" " THEN GOTO 3
10
300 C$=C$+MID$(M$,I,1)
310 IF I<>L THEN GOTO 330
320 B=LEN(C$)
330 MID$(A$,AS,1)="*"
340 NEXT I
350 IF MID$(M$,2,1)="S" THEN GOTO 600
360 D=INT(26/B)
362 IF B*D=26 THEN GOTO 365
364 D=D+1
365 LC=B*D
390 IF LC<=26 THEN GOTO 430
400 FOR I=27 TO LC
410 C$=C$+"*"
420 NEXT I
430 DIM A$(D,B)
435 W=1
440 FOR J=1 TO D
450 FOR I=1 TO B
460 A$(J,I)=MID$(C$,W,1)
465 W=W+1
470 NEXT I
480 NEXT J
490 C$=""
500 FOR I=1 TO B
510 FOR J=D TO 1 STEP -1
520 IF A$(J,I)="*" THEN GOTO 540
530 C$=C$+A$(J,I)
540 NEXT J
550 NEXT I
600 LOCATE 2,8:PRINT "TEXTO: ";
610 INPUT T$
620 IF MID$ (M$,1,1)="C" THEN LOCATE
```

```
2,13:PRINT "Texto cifrado: ";
630 IF T$="0" THEN GOTO 9999
640 LT=LEN(T$)
650 IF MID$(M$,1,1)="C" THEN GOTO 730
660 DIM P$(26)
670 FOR I=1 TO 26
675 G$=MID$(C$,I,1)
676 BZ=ASC(G$)
677 SE=BZ-CA
680 P$(SE)=CHR$(CA+I)
690 NEXT I
700 FOR I=1 TO 26
710 MID$(C$,I,1)=P$(I)
720 NEXT I
725 LOCATE 2,11:PRINT "Texto descifra
do: ";
730 FOR I=1 TO LT
740 IF MID$(T$,I,1)<"A" OR MID$(T$,I,
1)>"Z" THEN GOTO 770
750 PRINT MID$(C$,ASC(MID$(T$,I,1))-C
A,1);
760 GOTO 780
770 PRINT " ";
780 NEXT I
9999 END
```

PROGRAMA DE ANALISIS DE FRECUENCIAS

```
1 REM ****************************
2 REM *                          *
3 REM * ANALISIS DE FRECUENCIAS *
4 REM *                          *
5 REM ****************************
6 REM
10 CLEAR 2000
12 DIM E(26),D(26),T(26,26),F(26,26)
15 KEYOFF:CLS:POKE -853,255:OUT 170,2
55
16 PRINT TAB(1);"PROGRAMA DE ANALISIS
 DE FRECUENCIA"
30 LOCATE 0,5:PRINT "INTRODUCE EL TEX
TO: ";
40 INPUT T$
50 IF T$="0" THEN GOTO 9999
60 FOR I=1 TO LEN(T$)
70 IF I>LEN(T$) THEN GOTO 140
80 IF MID$(T$,I,1)>="A" AND MID$(T$,I
,1)<="Z" THEN GOTO 140
90 R$=""
100 IF I>1 THEN R$=MID$(T$,1,I-1)
110 IF I<LEN(T$) THEN R$=R$+MID$(T$,I
+1)
120 T$=R$
130 GOTO 70
140 NEXT I
150 LT=LEN(T$)
160 IF LT>3 THEN GOTO 190
170 LOCATE 0,5:PRINT "?":FOR TT=1 TO
10:BEEP:NEXT TT:LOCATE 0,5:PRINT " "
180 GOTO 30
190 CLS:LOCATE 2,2:PRINT "TEXTO: ";T$
200 GOSUB 8000
210 CA=ASC("A")-1
230 PRINT TAB(2);"FRECUENCIA RELATIVA
 DE LAS LETRAS":LOCATE 0,4
240 FOR I=1 TO LT
250 E(ASC(MID$(T$,I,1))-CA)=E(ASC(MID
$(T$,I,1))-CA)+1
260 NEXT I
270 FOR I=1 TO 26
275 IF I=>14 THEN LOCATE 19,I-10
280 PRINT CHR$(I+CA);": ";:PRINT USIN
G "###.############";(E(I)/LT)*100;:PRI
NT CHR$(6)
290 NEXT I
300 GOSUB 8000
310 PRINT TAB(10);"LETRAS REPETIDAS"
320 FOR I=1 TO LT-1
330 IF MID$(T$,I,1)=MID$(T$,I+1,1) TH
EN D(ASC(MID$(T$,I,1))-CA)=D(ASC(MID$
(T$,I,1))-CA)+1
340 NEXT I
350 LOCATE 0,4
360 FOR I=1 TO 26
365 IF I=>14 THEN LOCATE 19,I-10
370 PRINT CHR$(I+CA);":";D(I);CHR$(6)
380 NEXT I
390 GOSUB 8000
400 PRINT "FRECUENCIA DE DOS LETRAS C
ONSECUTIVAS":LOCATE 0,4
420 FOR I=1 TO LT-1
430 T(ASC(MID$(T$,I,1))-CA,ASC(MID$(T
$,I+1,1))-CA)=T(ASC(MID$(T$,I,1))-CA,
ASC(MID$(T$,I+1,1))-CA)+1
440 NEXT I
450 FOR I=1 TO 26
460 FOR J=1 TO 26
470 IF T(I,J)>0 THEN PRINT CHR$(I+CA)
;CHR$(J+CA);":";T(I,J);CHR$(6):CC=CC+
1
```

```
480 YY=CSRLIN:IF YY=15 THEN GOSUB 800
0
490 NEXT J
500 NEXT I
510 GOSUB 8000
520 PRINT TAB(7);"LETRAS EN ORDEN INV
ERSO":LOCATE 0,4
530 FOR I=1 TO 26
540 FOR J=1 TO 26
550 IF T(I,J)>0 AND T(J,I)>0 AND I<>J
 AND F(I,J)=0 AND F(J,I)=0 THEN PRINT
 CHR$(I+CA);CHR$(J+CA);":";T(I,J);:PR
INT TAB(10);CHR$(J+CA);CHR$(I+CA);":"
;T(J,I):F(I,J)=1
560 YY=CSRLIN:IF YY=22 THEN GOSUB 800
0
570 NEXT J
580 NEXT I
590 GOSUB 8000
595 PRINT "PROBABILIDAD DE CONTACTO L.
ADO DERECHO":LOCATE 0,4
610 FOR I=1 TO 26
620 IF E(I)=0 THEN GOTO 660
630 FOR J=1 TO 26
640 F(I,J)=T(I,J)/E(I)
650 NEXT J
660 NEXT I
680 FOR I=1 TO 26
690 FOR J=1 TO 26
700 IF F(I,J)>0 THEN PRINT CHR$(I+CA)
;CHR$(J+CA);":";:PRINT USING "###.##"
;F(I,J)*100;:PRINT CHR$(6)
710 YY=CSRLIN:IF YY=15 THEN GOSUB 800
0
720 NEXT J
730 NEXT I
740 GOSUB 8000
745 PRINT "PROBABILIDAD CONTACTO LADO
 IZQUIERDO":LOCATE 0,4
760 FOR I=1 TO 26
770 IF E(I)=0 THEN GOTO 810
780 FOR J=1 TO 26
790 F(I,J)=T(J,I)/E(I)
800 NEXT J
810 NEXT I
830 FOR I=1 TO 26
840 FOR J=1 TO 26
850 IF F(I,J)>0 THEN PRINT CHR$(J+CA)
;CHR$(I+CA);":";:PRINT USING "###.##"
;F(I,J)*100;:PRINT CHR$(6)
860 YY=CSRLIN:IF YY=15 THEN GOSUB 800
0
870 NEXT J
880 NEXT I
890 GOSUB 8000
895 PRINT TAB(13);"TRIGRAMAS":LOCATE
0,4
900 DIM G%(26,LT)
910 FOR I=1 TO 26
920 FOR J=2 TO LT-1
930 IF MID$(T$,J,1)=CHR$(I+CA) THEN G
%(I,J)=1
940 NEXT J
950 NEXT I
970 FOR I=1 TO 26
980 IF E(I)=0 OR (E(I)=1 AND (MID$(T$
,1,1)=CHR$(I+CA) OR MID$(T$,LT,1)=CHR
$(I+CA))) THEN GOTO 1050
990 PRINT CHR$(I+CA);":";
1000 FOR J=2 TO LT
1010 IF G%(I,J)=1 THEN PRINT MID$(T$,
J-1,3);",";
1020 NEXT J
1030 PRINT CHR$(8);" "
1040 YY=CSRLIN:IF YY=19 THEN GOSUB 80
00
1050 NEXT I
1060 GOSUB 8000
1070 GOTO 9999
8000 LOCATE 5,19:PRINT "PULSE LA BARR
A ESPACIADORA":PRINT TAB(12);"PARA SE
GUIR":PRINT "(PARA SALIDA POR IMPRESO
RA PULSE <C>)"
8010 R$=INKEY$
8020 IF R$="" THEN GOTO 8010
8025 IF R$="C" THEN GOTO 8085
8060 IF R$="0" THEN GOTO 9999
8070 CLS
8080 RETURN
8081 REM ************************
8082 REM RUTINA PARA LA IMPRESORA
8085 A$=""
8095 A%=BASE(0)
8105 B%=BASE(2)
8115 OPEN "LPT:" AS #1
8125 FOR I%=A% TO A%+960
8135 C%=VPEEK(I%):A$=A$+CHR$(C%)
8145 IF LEN(A$)=40 THEN PRINT #1,A$:A
$=""
8155 NEXT I%
8165 CLOSE #1
8170 GOTO 8010
9999 END
```

AYUDA MONOALFABETICA

```
1 REM ************************
2 REM *                      *
3 REM * AYUDA MONOALFABETICA *
4 REM *                      *
5 REM ************************
6 REM
10 KEYOFF:CLEAR 2000:POKE -853,0:CLS
15 DIM E(26),T(26,26),N(26)
20 COLOR 1,4,4:LOCATE 7,11:PRINT "PON
GA LA CINTA CON DATOS":LOCATE 4,12:PR
INT "Y LUEGO PULSE CUALQUIER TECLA"
30 BEEP:BEEP:BEEP
40 IF INKEY$="" THEN GOTO 40
45 OPEN "CAS:FRECUENCIAS" FOR INPUT A
S#1
47 FOR A=1 TO 26:INPUT #1,E(A):E(A)=E
(A)/100:NEXT A:CLOSE #1
50 OPEN "CAS:CONTACTOS" FOR INPUT AS#
1
60 FOR A=1 TO 26:FOR B=1 TO 26:INPUT
#1,T(A,B):NEXT B:NEXT A:CLOSE #1
70 CLS:COLOR 15,4,4
80 PRINT TAB(2);"PROGRAMA DE AYUDA MO
NOALFABETICA"
85 PRINT TAB(2);"==================
============"
90 LOCATE 2,2:PRINT "TEXTO: ";
100 INPUT T$
110 IF LEFT$(T$,1)="0" THEN GOTO 9999
120 LT=LEN(T$)
130 IF LT>9 THEN GOTO 160
140 LOCATE 13,20:PRINT "TEXTO CORTO":
FOR T=1 TO 10:BEEP:NEXT T:LOCATE 13,2
0:PRINT SPACE$(11)
150 GOTO 70
160 DIM T$(LT):FOR I=1 TO LT:T$(I)=MI
D$(T$,I,1):NEXT I
165 FOR I=1 TO LT
180 IF T$(I)<"a" OR T$(I)>"z" THEN T$
(I)=" "
200 NEXT I
230 GOSUB 8300
232 CLS:LOCATE 0,5:PRINT "TEXTO: ";T$
234 BL=6+INT((LT-1)/15)
236 DIM C(26)
238 CA=ASC("a")-1
240 FOR I=1 TO LT
245 IF T$(I)<>" " THEN C(ASC(T$(I))-C
A)=C(ASC(T$(I))-CA)+1/LT
250 NEXT I
260 GOSUB 8000
265 CLS
270 FOR I=1 TO 26
275 IF I<14 THEN LOCATE 0,I ELSE LOCA
TE 20,I-13
280 PRINT CHR$(I+CA);":";:PRINT USING
 "###.###########";C(I)*100
290 NEXT I
300 GOSUB 8000
310 DIM A$(26),B$(26),P$(LT)
315 FOR I=1 TO 26:A$(I)="*":B$(I)="*"
:NEXT I
320 CLS
380 LOCATE 3,6:PRINT "ABCDEFGHIJKLMNO
PQRSTUVWXYZ":LOCATE 3,7:FOR X=1 TO 26
:PRINT A$(X);:NEXT X:PRINT:PRINT
385 P$=""
390 FOR I=0 TO 15*INT((LT-1)/15) STEP
 15
400 J=15
410 IF I+J>LT THEN J=LT-I
415 GOSUB 8300
420 PRINT MID$(T$,I+1,J);TAB(16);CHR$
(124);TAB(18);
430 FOR W=1 TO J
440 C$=" "
450 IF T$(I+W)<>" " THEN C$=A$(ASC(T$
(I+W))-CA)
460 P$(I+W)=C$
470 PRINT C$;
480 NEXT W
485 PRINT
490 NEXT I
500 LOCATE 5,21:PRINT "PULSE B,C,D,E,
F,N,P,S,T o 0"
510 R$=INKEY$:IF R$="" THEN 510
520 IF R$<>"b" THEN GOTO 920
550 GOSUB 8100
560 GOSUB 8200
570 PRINT "FRECUENCIA(";CHR$(L+CA);")
=";INT(1000*C(L)+.5)/10;"%"
575 IF C(L)=0 THEN GOTO 910
580 B=1
590 FOR I=1 TO 26
600 IF ABS(E(I)-C(L))>B THEN GOTO 630
610 B=ABS(E(I)-C(L))
620 P=I
630 NEXT I
640 PRINT "SUGERENCIA: ";CHR$(P+CA)
650 FOR X=1 TO 26:N(X)=0:NEXT X
660 FOR I=2 TO LT
670 IF T$(I)<>L$ THEN GOTO 800
680 J=0
683 J=J+1
687 IF I-J<1 THEN GOTO 800
690 IF P$(I-J)="*" THEN GOTO 800
695 IF P$(I-J)=" " THEN GOTO 683
700 T=ASC(P$(I-J))-CA
710 FOR J=1 TO 26
720 N(J)=N(J)+T(T,J)
730 NEXT J
800 NEXT I
```

```
810 FOR I=2 TO (19-BL)*2
820 B=0
830 FOR J=1 TO 26
840 IF N(J)<=B THEN GOTO 870
850 B=N(J)
860 P=J
870 NEXT J
880 IF B=0 THEN GOTO 910
885 LOCATE 15,3
890 PRINT "CONTACTO: ";CHR$(P+CA);":"
;N(P)
895 N(P)=0
900 NEXT I
910 GOTO 500
920 IF R$<>"c" THEN GOTO 950
930 GOSUB 10000:REM
       RUTINA DE LA IMPRESORA
940 GOTO 500
950 IF R$<>"d" THEN GOTO 990
960 GOSUB 8200
965 IF A$(L)<>"*" THEN B$(ASC(A$(L))-
CA)="*"
970 A$(L)="*"
980 GOTO 320
990 IF R$<>"e" THEN GOTO 1040
1000 GOSUB 8100
1010 GOSUB 8200
1020 PRINT L$;":";E(L)
1030 GOTO 500
1040 IF R$<>"f" THEN GOTO 1090
1050 GOSUB 8100
1060 GOSUB 8200
1070 PRINT L$;":";C(L)
1080 GOTO 500
1090 IF R$<>"n" THEN GOTO 1100
1095 RUN
1100 IF R$<>"p" THEN GOTO 1200
1110 GOSUB 8100
1120 LOCATE 0,0:INPUT "LETRAS";L$
1130 IF L$="0" THEN GOTO 9999
1140 IF LEN(L$)<>2 THEN GOSUB 8100:GO
TO 1120
1150 L1=ASC(LEFT$(L$,1))-CA
1160 L2=ASC(RIGHT$(L$,1))-CA
1170 IF L1<1 OR L1>26 OR L2<1 OR L2>2
6 THEN GOTO 1120
1180 LOCATE 0,1:PRINT L$;":";T(L1,L2)
1190 GOTO 500
1200 IF R$<>"s" THEN GOTO 1240
1210 FOR I=9 TO 21
1213 LOCATE 0,I:PRINT TAB(37);" "
1217 NEXT I
1220 LOCATE 0,9:FOR X=1 TO LT:PRINT P
$(X);:NEXT X:PRINT
1230 GOTO 9999
1240 IF R$<>"t" THEN GOTO 1340
1250 GOSUB 8200
1260 Q$=L$
1270 LL=L
1280 LOCATE 12,1:GOSUB 8205
1300 IF B$(L)<>"*" THEN GOTO 1280
1310 IF A$(LL)<>"*" THEN B$(ASC(A$(LL
))-CA)="*"
1320 A$(LL)=L$
1325 B$(L)=Q$
1330 GOTO 320
1340 IF R$="0" THEN GOTO 9999
1350 LOCATE 0,21:PRINT "?";CHR$(7)
1370 GOTO 500
8000 LOCATE 8,20:PRINT "PULSE CUALQUI
ER TECLA"
8010 R$=INKEY$
8020 IF R$="" THEN GOTO 8010
8030 IF R$="0" THEN GOTO 9999
8040 LOCATE 0,20:PRINT SPACE$(37)
8050 RETURN
8100 LOCATE 0,0
8110 PRINT SPC(185)
8130 LOCATE 0,BL
8140 RETURN
8200 LOCATE 0,0
8201 PRINT SPC(185)
8202 LOCATE 0,0
8205 PRINT "LETRA:";:L$=INPUT$(1):PRI
NT L$
8210 IF LEFT$(L$,1)="0" THEN GOTO 999
9
8220 IF LEN(L$)<>1 THEN GOTO 8200
8230 L=ASC(L$)-CA
8240 IF L<1 OR L>26 THEN GOTO 8200
8250 RETURN
8300 T$="":FOR X=1 TO LT:T$=T$+T$(X):
NEXT X:RETURN
9999 END
10000 AA$=""
10010 A%=BASE(0)
10020 B%=BASE(2)
10030 OPEN "LPT:" AS #1
10040 FOR I%=A% TO A%+960
10050 C%=VPEEK(I%):AA$=AA$+CHR$(C%)
10060 IF LEN(AA$)=40 THEN PRINT #1,AA
$:AA$=""
10070 NEXT I%
10080 CLOSE #1
10090 RETURN
```

ZIG-ZAG

```
1 REM ***********
2 REM *         *
3 REM * ZIG-ZAG *
4 REM *         *
5 REM ***********
6 REM
10 KEYOFF:POKE -853,255:CLEAR 1000:CL
S:DIM C$(500)
20 PRINT TAB(4);"PROGRAMA DE CIFRADO
<ZIG-ZAG>"
30 LOCATE 2,2:PRINT "MODO Y CLAVE";
40 INPUT M$
50 IF M$="0" THEN GOTO  9999
60 IF LEN(M$)<2 THEN GOTO 110
70 IF LEFT$(M$,1)<"C" OR LEFT$(M$,1)>
"D" THEN GOTO 110
75 FOR I=2 TO LEN(M$)
80 IF MID$(M$,I,1)<"3" OR MID$(M$,I,1
)>"9" THEN GOTO 110
90 NEXT I
100 GOTO 130
110 LOCATE 0,2:PRINT "?":FOR T=1 TO 1
0:BEEP:NEXT T:LOCATE 0,2:PRINT " "
120 GOTO 30
130 K=VAL(MID$(M$,2,1))
140 IF K<3 THEN GOTO 110
145 LOCATE 0,2:PRINT SPC(37)
150 LOCATE 0,2:PRINT "MODO: ";LEFT$(M
$,1)
155 LOCATE 0,3:PRINT "CLAVE: ";K
156 PRINT "=========================
==========="
160 LOCATE 0,6:PRINT "TEXTO:";
170 INPUT T$
171 FOR I=2 TO LEN(T$)
172 IF I<LEN(T$) THEN IF MID$(T$,I,1)
=" " THEN T$=LEFT$(T$,I-1)+RIGHT$(T$,
LEN(T$)-I)
173 NEXT I
175 IF T$="0" THEN GOTO 9999
180 LT=LEN(T$)
190 IF LT>0 THEN GOTO 215
200 LOCATE 0,4:PRINT "?":FOR T=1 TO 1
0:BEEP:NEXT T:LOCATE 0,4:PRINT " "
210 GOTO 170
215 LOCATE 0,6:PRINT SPC(LEN(T$)+10)
220 LOCATE 0,6:PRINT "TEXTO: ";T$
230 PRINT
240 S=2*(K-1)
250 IF MID$(M$,1,1)="D" THEN GOTO 400
260 FOR I=1 TO LT STEP S
270 PRINT MID$(T$,I,1);
275 NEXT I
280 FOR I=1 TO K-2
290 FOR J=1 TO LT STEP S
300 IF J+1<=LT THEN PRINT MID$(T$,J+I
,1);
310 IF J+S-I<=LT THEN PRINT MID$(T$,J
+S-I,1);
330 NEXT J
340 NEXT I
350 FOR I=K TO LT STEP S
360 PRINT MID$(T$,I,1);
370 NEXT I
380 GOTO 9999
400 L=0
410 FOR I=1 TO LT STEP S
420 L=L+1
430 C$(I)=MID$(T$,L,1)
440 NEXT I
450 FOR I=1 TO K-2
460 FOR J=1 TO LT STEP S
470 IF J+I>LT THEN GOTO 500
480 L=L+1
490 C$(I+J)=MID$(T$,L,1)
500 IF J+S-I>LT THEN GOTO 530
510 L=L+1
520 C$(J+S-I)=MID$(T$,L,1)
530 NEXT J
540 NEXT I
560 FOR I=K TO LT STEP S
570 L=L+1
580 C$(I)=MID$(T$,L,1)
590 NEXT I
600 FOR I=1 TO L :PRINT C$(I);:NEXT I
610 LOCATE 2,20:PRINT TAB(5);"PULSE <
S> PARA SEGUIR Y <N>":PRINT TAB(11);"
PARA DETENERSE"
620 R$=INKEY$
630 IF R$="" THEN GOTO 620
640 IF R$="S" THEN GOTO 680
650 IF R$="N" THEN GOTO 9999
660 LOCATE 0,21:PRINT "?"
670 GOTO 620
680 K=K+1
685 IF K>9 THEN K=3
690 LOCATE 7,3:PRINT K
700 GOTO 215
9999 END
```

COLUMNAS COMPLETAS

```
1 REM **********************
2 REM *                        *
3 REM * COLUMNAS COMPLETAS *
4 REM *                        *
5 REM **********************
6 REM
10 KEYOFF:POKE -853,255:CLEAR 1000:CL
S
15 PRINT TAB(3);"==================
==========="
20 PRINT TAB(3);"CIFRADO POR COLUMNAS
 COMPLETAS"
25 PRINT TAB(3);"==================
==========="
30 LOCATE 2,4:INPUT "MODO Y CLAVE:";M
C$
40 IF LEN(MC$)<3 THEN GOTO 30
50 IF LEFT$(MC$,1)<>"C" AND LEFT$(MC$
,1)<>"D" THEN GOTO 30
60 M$=LEFT$(MC$,1)
70 C$=MID$(MC$,2)
110 LC=LEN(C$)
120 DIM K(LC),CM$(LC)
121 FOR M=1 TO LC
122 CM$(M)=MID$(C$,M,1)
123 NEXT M
130 FOR I=1 TO LC
140 B$="^"
150 FOR J=1 TO LC
160 IF CM$(J)>=B$ THEN GOTO 200
180 B$=CM$(J)
190 P=J
200 NEXT J
210 CM$(P)="^"
216 K(I)=P
217 NEXT I
220 CLS
221 PRINT TAB(10);"MODO:";M$
230 PRINT TAB(10);"CLAVE:";C$
232 PRINT:PRINT "==================
==============="
240 PRINT:INPUT "TEXTO:";T$
250 FOR I=1 TO LEN(T$)
260 IF I>=LEN(T$) THEN GOTO 300
270 IF MID$(T$,I,1)<>" " THEN GOTO 30
0
275 IF I=1 THEN T$=RIGHT$(T$,LEN(T$)-
1):GOTO 290
280 T$=LEFT$(T$,I-1)+RIGHT$(T$,LEN(T$
)-I)
290 GOTO 260
300 NEXT I
310 IF LEFT$(T$,1)="0" THEN GOTO 9999
320 IF LEN(T$)>0 THEN GOTO 350
340 GOTO 230
350 LT=LEN(T$)
360 IF(LT/LC)=INT(LT/LC) THEN GOTO 39
0
370 T$=T$+CHR$(65+INT(26*RND(-TIME)))
380 GOTO 350
390 PRINT:PRINT "TEXTO:";T$
400 PRINT
401 DIM TM$(LT)
402 FOR M=1 TO LT
403 TM$(M)=MID$(T$,M,1)
404 NEXT M
410 IF LEFT$(M$,1)="D" THEN GOTO 480
420 H=0
425 FOR I=1 TO LC
430 FOR J=K(I) TO LT STEP LC
435 H=H+1
440 PRINT TM$(J);
445 IF H/5=INT(H/5) THEN PRINT " ";
450 NEXT J
460 NEXT I
470 GOTO 9999
480 DIM CB$(LT)
481 FOR H=1 TO LT
482 IF H>LC THEN GOTO 489
483 CB$(H)=CM$(H)
489 NEXT H
490 L=0
500 FOR I=1 TO LC
510 FOR J=K(I) TO LT STEP LC
520 L=L+1
521 IF L>LT THEN GOTO 540
530 CB$(J)=TM$(L)
540 NEXT J
550 NEXT I
560 FOR H=1 TO LT
570 PRINT CB$(H);
575 IF C$="C" AND H/5=INT(H/5) THEN P
RINT D ";
580 NEXT H
9999 END
```

TRANSPOSICION DE ITINERARIO

```
1 REM ********************************
2 REM *                              *
3 REM * TRANSPOSICION DE ITINERARIO *
4 REM *                              *
5 REM ********************************
6 REM
10 DIM L$(50),C$(25)
20 KEYOFF:POKE -853,255:OUT 170,0:MOT
OR:CLS
22 INPUT "LEO DATOS DE LA CINTA";R$
24 IF R$="S" THEN GOTO 1600
30 FOR R=1 TO 32
40 READ L$(R)
50 NEXT R
60 DATA "AFKPUBGLQVCHMRWDINSXEJOTY"
70 DATA "UPKFAVQLGBWRMHCXSNIDYTOJE"
80 DATA "EJOTYDINSXCHMRWBGLQVAFKPU"
90 DATA "YTOJEXSNIDWRMHCVQLGBUPKFA"
100 DATA "ABCDEFGHIJKLMNOPQRSTUVWXY"
110 DATA "UVWXYPQRSTKLMNOFGHIJABCDE"
120 DATA "EDCBAJIHGFONMLKTSRQPYXWVU"
130 DATA "YXWVUTSRQPONMLKJIHGFEDCBA"
140 DATA "OSVXYJNRUWFIMQTCEHLPABDGK"
150 DATA "OJFCASNIEBVRMHDXUQLGYWTPK"
160 DATA "ACFJOBEINSDHMRVGLQUXKPTWY"
170 DATA "YXVSOWURNJTQMIFPLHECKGDBA"
180 DATA "KPTWYGLQUXDHMRVBEINSACFJO"
190 DATA "KGDBAPLHECTQMIFWURNJYXVSO"
200 DATA "ABDGKCEHLPFIMQTJNRUWOSVXY"
210 DATA "YWTPKXUQLGVRMHDSNIEBOJFCA"
220 DATA "EFOPYDGNQXCHMRWBILSVAJKTU"
230 DATA "YPOFEXQNGDWRMHCVSLIBUTKJA"
240 DATA "AJKTUBILSVCHMRWDGNQXEFOPY"
250 DATA "UTKJAVSLIBWRMHCXQNGDYPOFE"
260 DATA "ABCDEJIHGFKLMNOTSRQPUVWXY"
270 DATA "UVWXYTSRQPKLMNOJIHGFABCDE"
280 DATA "EDCBAFGHIJONMLKPQRSTYXWVU"
290 DATA "YXWVUPQRSTONMLKFGHIJEDCBA"
300 DATA "ABFGOCEHNPDIMQVJLRUWKSTXY"
310 DATA "YXTSKWURLJVQMIDPNHECOGFBA"
320 DATA "ACDJKBEILSFHMRTGNQUXOPVWY"
330 DATA "YWVPOXUQNGTRMHFSLIEBKJDCA"
340 DATA "OPVWYGNQUXFHMRTBEILSACDJK"
350 DATA "KJDCASLIEBTRMHFXUQNGYWVPO"
360 DATA "KSTXYJLRUWDIMQVCEHNPABFGO"
370 DATA "OGFBAPNHECVQMIDWURLJYXTSK"
377 CA=ASC("A")-1
380 SS$="":CLS
390 PRINT TAB(5);"TRANSPOSICION DE IT
INERARIO"
391 PRINT TAB(5);"==================
========"
400 LOCATE 2,2:PRINT"MODO:";
410 INPUT M$
420 IF M$="0" GOTO 9999
430 IF M$="L" GOTO 1010
440 IF M$="S" GOTO 1510
450 IF M$<"C" OR M$>"D" THEN GOTO 400
460 LOCATE 2,3:INPUT "NUMERO CLAVE:";
NC$
470 IF LEN(NC$)<1 THEN END:GOTO 400
471 F=0
480 FOR I=1 TO LEN(NC$)
490 N1C$=MID$(NC$,I,1)
495 IF N1C$<"0" OR N1C$>"9" THEN F=1
500 NEXT I
505 IF F=1 THEN GOTO 400
510 K=VAL(NC$)
520 IF K<1 OR MID$(L$(K),10)="" THEN
GOTO 400
530 PRINT:PRINT "ITINERARIO:"
535 PRINT
540 FOR Y=0 TO 4
550 PRINT MID$(L$(K),Y*5+1,5)
560 NEXT Y
570 PRINT:INPUT "TEXTO ";T$
590 FOR I=1 TO LEN(T$)
600 IF I>LEN(T$) THEN GOTO 670
610 T1$=MID$(T$,I,1)
615 IF T1$<>" " THEN GOTO 670
620 R$=""
630 IF I>1 THEN R$=LEFT$(T$,I-1)
640 IF I<LEN(T$) THEN R$=R$+RIGHT$(T$
,LEN(T$)-I)
650 T$=R$
660 GOTO 600
670 NEXT I
680 IF LEFT$(T$,1)="0" THEN GOTO 9999
690 LT=LEN(T$)
700 IF LT>0 THEN GOTO 730
710 GOTO 570
730 IF LT/25=INT(LT/25) THEN GOTO 770
740 T$=T$+"Z"
750 LT=LT+1
760 GOTO 730
770 PRINT:PRINT "TEXTO: ";T$
780 PRINT
790 IF M$="D" THEN GOTO 910
800 PRINT "CIFRADO: ";
810 FOR I=1 TO 25
820 FOR J=1 TO 25
830 IF MID$(L$(K),J,1)=CHR$(CA+I) THE
N C$(J)=MID$(T$,I,1)
840 NEXT J
850 NEXT I
860 FOR S=1 TO 25
861 PRINT C$(S);
862 NEXT S
```

```
870 IF LT=25 THEN GOTO 9995
880 T$=RIGHT$(T$,LEN(T$)-25)
890 LT=LT-25
900 GOTO 810
910 PRINT "DESCIFRADO: ";
920 FOR I=1 TO 25
930 FOR J=1 TO 25
940 IF MID$(L$(K),J,1)=CHR$(CA+I) THE
N C$(I)=MID$(T$,J,1)
950 NEXT J
960 NEXT I
970 FOR I=1 TO 25
971 PRINT C$(I);
972 NEXT I
975 IF LT=25 THEN GOTO 9995
980 T$=RIGHT$(T$,LEN(T$)-25)
990 LT=LT-25
1000 GOTO 920
1010 IF R<=50 THEN GOTO 1070
1020 LOCATE 0,4:PRINT"LIBRERIA COMPLE
TA"
1030 PRINT CHR$(7)
1040 GOTO 400
1070 LOCATE 0,2:PRINT"RUTA NUMERO";R
1080 FOR X=0 TO 4
1090 LOCATE 0,X+14:INPUT M$(X)
1100 IF LEN(M$(X))<>5 THEN GOTO 1090
1110 FOR Y=1 TO 5
1120 IF (MID$(M$(X),Y,1)<"A") OR (MID
$(M$(X),Y,1)>"Z") THEN GOTO 1090
1130 NEXT Y
1140 NEXT X
1150 C$=""
1160 FOR X=0 TO 4
1170 C$=C$+M$(X)
1180 NEXT X
1190 FOR X=2 TO 25
1200 FOR Y=1 TO X-1
1210 IF MID$(C$,X,1)=MID$(C$,Y,1) THE
N GOTO 1080
1220 NEXT Y
1230 NEXT X
1240 L$(R)=C$
1495 R=R+1
1500 GOTO 380
1510 CLS
1520 LOCATE 0,10:INPUT "CON QUE NOMBR
E QUIERES SALVARLO";N$
1530 R$="CAS:"+N$:OPEN R$ FOR OUTPUT
AS #1
1540 FOR I=1 TO 50:PRINT #1,L$(I):NEX
T I
1550 CLOSE #1
1590 GOTO 377
1600 CLS:INPUT "NOMBRE DEL FICHERO";N
$
1610 R$="CAS:"+N$:OPEN R$ FOR INPUT A
S #1
1620 FOR I=1 TO 50:INPUT #1,L$(I):NEX
T I
1630 CLOSE #1
1640 GOTO 377
9995 PRINT:PRINT:PRINT TAB(11);"QUIER
ES SEGUIR?":BEEP
9996 SS$=INKEY$:IF SS$="" THEN 9996
9997 IF SS$="S" THEN 380
9999 END
```

REJILLA DE CARDANO

```
1 REM **********************
2 REM *                      *
3 REM * REJILLA DE CARDANO *
4 REM *                      *
5 REM **********************
6 REM
10 KEYOFF:CLEAR 1000:POKE -853,255:OU
T 170,0:MOTOR:CLS
20 PRINT TAB(4);"CIFRADO <REJILLA DE
CARDANO>"
25 PRINT TAB(4);STRING$(28,61)
30 LOCATE 2,2:PRINT "MODO:";:M$=INPUT
$(1)
40 IF M$="0" THEN GOTO 9999
50 IF M$="C" OR M$="D" THEN GOTO 90
70 LOCATE 7,2:PRINT "?":FOR T=1 TO 10
:BEEP:NEXT T:LOCATE 7,2:PRINT " "
80 GOTO 30
90 LOCATE 2,2:PRINT "MODO:";M$
93 DIM G(6,6)
97 NH=0
190 FOR Q=1 TO 4
200 SX=24
210 IF Q=2 OR Q=3 THEN SX=28
220 SY=3
230 IF Q>2 THEN SY=7
240 LOCATE SX,SY:PRINT "123";:LOCATE
SX,SY+1:PRINT "456";:LOCATE SX,SY+2:P
RINT "789"
250 LOCATE 1,4:PRINT "CUADRANTE";Q;"A
GUJERO ";
260 R$=INPUT$(1):PRINT R$
280 IF R$="" THEN GOTO 250
290 IF R$="0" THEN GOTO 9999
300 IF R$="N" THEN GOTO 620
310 IF R$>="1" AND R$<="9" THEN GOTO
350
320 LOCATE 21,4:PRINT "?":FOR T=1 TO
```

```
10:BEEP:NEXT T:LOCATE 21,4:PRINT " "
340 GOTO 250
350 V=VAL(R$)
370 GY=INT((V-1)/3)+1
380 GX=V-3*(GY-1)
390 IF Q=2 OR Q=3 THEN GX=GX+3
400 IF Q>2 THEN GY=GY+3
410 IF G(GY,GX)=1 THEN GOTO 320
420 FOR Y=1 TO 6
430 FOR X=1 TO 6
440 IF G(Y,X)=0 THEN GOTO 530
450 YY=Y
460 XX=X
470 FOR R=1 TO Q-1
480 I=YY
490 YY=XX
500 XX=7-I
510 IF YY=GY AND XX=GX THEN GOTO 320
520 NEXT R
530 NEXT X
540 NEXT Y
550 G(GY,GX)=1
560 IF GX>3 THEN GX=GX+1
570 IF GY>3 THEN GY=GY+1
580 LOCATE GX+23,GY+2:PRINT CHR$(219)
590 NH=NH+1
600 IF NH<9 THEN GOTO 250
610 Q=4
620 IF Q=4 AND NH<9 THEN GOTO 320
680 NEXT Q
690 LOCATE 0,4:PRINT SPC(23)
700 LOCATE 2,12:PRINT "TEXTO:";
710 INPUT "";T$
715 IF LEN(T$)<1 THEN 700
720 FOR I=1 TO LEN(T$)
730 IF I>LEN(T$) THEN GOTO 800
740 IF MID$(T$,I,1)<>" " THEN GOTO 80
0
750 R$=""
760 IF I>1 THEN R$=LEFT$(T$,I-1)
770 IF I<LEN(T$) THEN R$=R$+RIGHT$(T$
,LEN(T$)-I)
780 T$=R$
790 GOTO 730
800 NEXT I
810 IF T$="0" THEN GOTO 9999
820 LT=LEN(T$)
830 IF LT/36=INT(LT/36) THEN GOTO 870
840 T$=T$+"Z"
850 LT=LT+1
860 GOTO 830
870 LOCATE 0,12:PRINT SPC(LEN(T$)+11)
875 LOCATE 0,12:PRINT "TEXTO: ";T$
880 PRINT
890 DIM C$(6,6)
895 RF=1
900 IF M$="D" THEN GOTO 1110
910 CN=0
920 FOR Q=1 TO 4
930 FOR Y=1 TO 6
940 FOR X=1 TO 6
950 IF G(Y,X)=0 THEN GOTO 980
960 CN=CN+1
970 C$(Y,X)=MID$(T$,CN,1)
980 NEXT X
990 NEXT Y
1000 GOSUB 2000
1010 NEXT Q
1020 FOR Y=1 TO 6
1030 FOR X=1 TO 6
1040 PRINT C$(Y,X);
1050 NEXT X
1060 NEXT Y
1070 IF LT=36 THEN GOTO 9999
1080 T$=RIGHT$(T$,LEN(T$)-36)
1090 LT=LT-36
1100 GOTO 910
1110 CN=0
1120 FOR Y=1 TO 6
1130 FOR X=1 TO 6
1140 CN=CN+1
1150 C$(Y,X)=MID$(T$,CN,1)
1160 NEXT X
1170 NEXT Y
1180 FOR Q=1 TO 4
1190 FOR Y=1 TO 6
1200 FOR X=1 TO 6
1210 IF G(Y,X)>0 THEN PRINT C$(Y,X);
1220 NEXT X
1230 NEXT Y
1240 GOSUB 2000
1250 NEXT Q
1260 IF LT=36 THEN GOTO 9999
1270 T$=RIGHT$(T$,LEN(T$)-36)
1280 LT=LT-36
1290 GOTO 1110
2000 FOR Y=1 TO 6
2010 FOR X=1 TO 6
2020 IF G(Y,X)<>RF THEN GOTO 2070
2030 G(Y,X)=0
2040 YY=X
2050 XX=7-Y
2060 G(YY,XX)=3-RF
2070 NEXT X
2080 NEXT Y
2090 RF=3-RF
2100 RETURN
9999 END
1314 L2=ASC(RIGHT$(R$,1))-CA
1315 IF L1<1 OR L1>26 OR L2<1 OR L2>2
6 THEN GOTO 1311
1316 LOCATE 14,21:PRINT "FREC=";T(L1,
L2)
1318 GOTO 840
1319 IF R$="S" THEN GOTO 1350
1320 LOCATE 0,20:PRINT "?":FOR T=1 TO
 10:BEEP:NEXT T:LOCATE 0,20:PRINT " "
1330 BEEP:BEEP:BEEP
1340 GOTO 840
1350 CLS:PRINT TAB(4);"SOLUCION:"
1360 FOR J=1 TO NR
1365 FOR I=1 TO NC
```

```
1370 PRINT C$(J,B(I));
1380 NEXT I:NEXT J
1390 GOTO 9999
8000 LOCATE 0,16:INPUT "QUE COLUMNA Q
UIERE PONER";CN
8010 CN=INT(CN)
8020 IF CN=0 THEN GOTO 9999
8030 IF CN<1 OR CN>NC THEN GOTO 8000
8035 IF F(CN)>0 THEN GOTO 8000
8040 RETURN
8050 LOCATE 0,15:INPUT "POSICION";PC
8055 LOCATE 0,15:PRINT SPC(40)
8060 PC=INT(PC)
8070 IF PC=0 THEN GOTO 9999
8080 IF PC<1 OR PC>NC THEN GOTO 8050
8090 RETURN
8100 FOR I=1 TO NR:FOR J=1 TO NC:P$(I
,J)=" ":NEXT J:NEXT I
8110 FOR I=1 TO NC
8115 LOCATE I,3:PRINT "-"
8120 C=F(I)
8130 IF C=0 THEN GOTO 8170
8135 LOCATE I,3:PRINT CHR$(219)
8140 FOR J=1 TO NR
8150 P$(J,C)=C$(J,I)
8160 NEXT J
8170 NEXT I
8180 FOR I=1 TO NR
8190 LOCATE 17,3+I:FOR J=1 TO NC:PRIN
T P$(I,J);:NEXT J:PRINT
8200 NEXT I
8210 RETURN
8220 SY=NR+4
8230 FOR I=SY TO 20
8240 LOCATE 0,I:PRINT TAB(31);" "
8250 NEXT I
8260 RETURN
9999 END
10000 REM RUTINA PARA LA IMPRESORA
10010 AA$=""
10020 A%=BASE(0)
10030 B%=BASE(2)
10040 OPEN "LPT:" AS #1
10050 FOR I%=A% TO A%+960
10060 C%=VPEEK(I%):AA$=AA$+CHR$(C%)
10070 IF LEN (AA$)=40 THEN PRINT #1,A
A$:AA$=""
10080 NEXT I%
10090 CLOSE #1
10100 RETURN
```

ANALISIS POR COLUMNAS COMPLETAS

```
1 REM ************************
2 REM *                      *
3 REM * ANALISIS POR COLUMNAS *
4 REM *        COMPLETAS     *
5 REM *                      *
6 REM ************************
7 REM
10 SCREEN 0:POKE -853,255:OUT 170,255
:CLEAR 2000:KEY OFF
15 NR=30:NC=15:DIM C$(NR,NC),P$(NR,NC
),B(NC),F(NC),E(26),T(26,26)
17 D$=CHR$(4)
20 LOCATE 6,11:PRINT "PONGA LA CINTA
CON DATOS":LOCATE 4,12:PRINT "Y LUEGO
 PULSE CUALQUIER TECLA"
30 BEEP:BEEP:BEEP
40 IF INKEY$="" THEN GOTO 40
50 OPEN "CAS:FRECUENCIAS" FOR INPUT A
S#1
55 FOR A=1 TO 20:INPUT #1,E(A):E(A)=E
(A)*100):NEXT A
60 CLOSE #1
65 OPEN "CAS:CONTACTOS" FOR INPUT AS#
1
70 FOR A=1 TO 26:FOR B=1 TO 26:INPUT
#1,T(A,B):T(A,B)=T(A,B)*100:NEXT B:NE
XT A
75 CLOSE #1
80 CLS
85 PRINT TAB(3);"ANALISIS FOR COLUMNA
S COMPLETAS"
86 PRINT TAB(3);STRING$(31,61)
90 LOCATE 2,2:PRINT "TEXTO: ";
100 INPUT T$
110 FOR I=1 TO LEN(T$)
120 IF I>LEN(T$) THEN GOTO 190
130 IF MID$(T$,I,1)<>" " THEN GOTO 19
0
140 R$=""
150 IF I>1 THEN R$=LEFT$(T$,I-1)
160 IF I<LEN(T$) THEN R$=R$+RIGHT$(T$
,LEN(T$)-I)
170 T$=R$
180 GOTO 120
190 NEXT I
200 IF T$="0" THEN GOTO 9999
210 LT=LEN(T$)
220 IF LT>0 THEN GOTO 250
230 LOCATE 0,2:PRINT "?":FOR T=1 TO 1
0:BEEP:NEXT T:LOCATE 0,2:PRINT " "
```

```
240 GOTO 90
250 NF=0
260 FOR I=2 TO INT(LT/2)
270 IF LT/I=INT(LT/I) THEN NF=NF+1
280 NEXT I
290 IF NF=0 THEN GOTO 230
300 DIM C(NF)
310 DIM R(NF)
320 NF=0
330 FOR I=2 TO INT(LT/2)
340 IF LT/I>INT(LT/I) THEN GOTO 380
350 NF=NF+1
360 C(NF)=I
370 R(NF)=LT/I
380 NEXT I
385 CA=ASC("A")-1
390 CLS:LOCATE 0,2:PRINT "TEXTO: ";T$
400 PRINT
410 PRINT "HAY";NF;"MODOS POSIBLES DE
 FACTORIZACION"
420 PRINT
430 FOR I=1 TO NF
440 PRINT I;":";R(I);"filas,";C(I);"c
olumnas."
445 NEXT I
450 PRINT
460 PRINT TAB(1);"DISTRIBUCION DE VOC
ALES (S/N/0) ?";
480 R$=INKEY$
490 IF R$="" THEN GOTO 480
500 IF R$="0"THEN 9999
505 IF R$="C" THEN GOSUB 10000:CLS:GO
TO 450
510 IF R$="N" THEN GOTO 650
515 CLS
520 FOR I=1 TO NF
530 PRINT I;":";C(I);"x";R(I);":";
540 FOR J=1 TO R(I)
550 NV=0
560 FOR K=1 TO C(I)
570 R$=MID$(T$,(K-1)*R(I)+J,1)
580 IF R$="A" OR R$="E" OR R$="I" OR
R$="O" OR R$="U" THEN NV=NV+1
590 NEXT K
600 PRINT INT(NV/C(I)*100);"%";
610 NEXT J
620 PRINT
630 PRINT
640 NEXT I
650 PRINT
660 INPUT "NUMERO DEL BLOQUE DE DIMEN
SIONES";R$
663 IF R$="C" THEN GOSUB 10000:GOTO 6
60
665 BD=VAL(R$)
667 IF BD=0 THEN 9999
670 IF BD<1 OR (BD>NF) OR BD>INT(BD)
THEN GOTO 660
680 NC=C(BD)
690 NR=R(BD)
692 FOR I=1 TO NR
693 FOR J=1 TO NC
694 C$(I,J)=MID$(T$,(J-1)*NR+I,1)
695 NEXT J
696 NEXT I
697 FOR I=1 TO NC:F(I)=0:B(I)=0:NEXT
I
700 CLS
710 FOR I=1 TO NC
720 LOCATE I,1:PRINT MID$(STR$(INT(I/
10)),2,1);:LOCATE 16+I,1:PRINT MID$(S
TR$(INT(I/10)),2,1)
730 LOCATE I,2:PRINT MID$(STR$(I-10*I
NT(I/10)),2,1);:LOCATE 16+I,2:PRINT M
ID$(STR$(I-10*INT(I/10)),2,1)
740 LOCATE I,3:PRINT "-":LOCATE 16+I,
3:PRINT "-"
750 NEXT I
760 FOR I=1 TO NR
770 FOR J=1 TO NC:PRINT TAB(1);C$(I,J
);:NEXT J:PRINT
780 NEXT I
790 GOSUB 8000
810 F(CN)=1
820 B(1)=CN
830 GOSUB 8100
840 LOCATE 0,20:PRINT TAB(36):LOCATE
5,20:PRINT "PULSE C,W,D,I,L,R,P,B,S o
 0"
845 LOCATE 0,21:PRINT TAB(36)
850 R$=INKEY$
860 IF R$="" THEN GOTO 850
867 IF R$="B" THEN CLS:GOTO 390
870 IF R$="C" THEN GOSUB 10000:GOTO 8
40
890 IF R$="0" THEN GOTO 9999
900 IF R$<>"L" AND R$<>"R" THEN GOTO
1160
910 GOSUB 8050
915 IF B(PC)=0 THEN GOTO 910
920 C=B(PC)
930 GOSUB 8220
1010 FOR I=1 TO NC
1020 IF I=C THEN GOTO 1140
1030 PRINT I;
1050 PRINT ":";
1060 P=0
1070 FOR J=1 TO NR
1080 CP=ASC(C$(J,C))-CA
1090 TC=ASC(C$(J,I))-CA
1100 IF R$="L" THEN P=P+T(TC,CP)
1110 IF R$="R" THEN P=P+T(CP,TC)
1120 NEXT J
1130 PRINT P;
1135 PRINT
1140 NEXT I
1150 IF PEEK(23689)>3 THEN GOTO 840
1151 INPUT "PULSE <RETURN>:";R$
1152 GOSUB 8220
1153 GOTO 840
1160 IF R$<>"D" THEN GOTO 1250
1170 GOSUB 8050
```

```
1175 IF B(PC)>0 THEN F(B(PC))=0:B(PC)
=0
1180 FOR I=PC TO NC-1
1190 B(I)=B(I+1)
1200 IF B(I)>0 THEN F(B(I))=I
1210 NEXT I
1220 B(NC)=0
1230 GOSUB 8100
1240 GOTO 840
1250 IF R$<>"I" THEN GOTO 1301
1255 GOSUB 8050
1257 F(B(NC))=0
1259 IF PC>=NC THEN GOTO 1290
1260 FOR I=NC TO PC+1 STEP -1
1270 B(I)=B(I-1)
1280 IF B(I)>0 THEN F(B(I))=I
1285 NEXT I
1292 B(PC)=0
1294 GOSUB 8100
1300 GOTO 840
1301 IF R$<>"W" THEN GOTO 1310
1302 GOSUB 8050
1303 GOSUB 8000
1304 IF B(PC)>0 THEN F(B(PC))=0
1305 F(CN)=PC
1306 B(PC)=CN
1307 GOSUB 8100
1308 GOTO 840
1310 IF R$<>"P" THEN GOTO 1319
1311 LOCATE 2,20:INPUT "LETRAS: ";R$
1312 IF LEN(R$)<>2 THEN GOTO 1311
1313 L1=ASC(LEFT$(R$,1))-CA
```

ANALISIS POR LA REJILLA DE CARDANO

```
1 REM ****************************
2 REM *                          *
3 REM * ANALISIS POR LA REJILLA *
4 REM *        DE CARDANO        *
5 REM *                          *
6 REM ****************************
7 REM
10 KEYOFF:POKE -853,255:CLS
15 DIM E(26),T(26,26),G(6,6),A(6,6)
20 LOCATE 6,11:PRINT "PONGA LA CINTA
CON DATOS":LOCATE 4,12:PRINT "Y LUEGO
 PULSE CUALQUIER TECLA"
30 BEEP:BEEP:BEEP
40 IF INKEY$="" THEN GOTO 40
50 OPEN "CAS:CONTACTOS" FOR INPUT AS
#1
53 FOR A=1 TO 26:INPUT #1,E(A):E(A)=E
(A)*100:NEXT A
55 CLOSE #1
58 OPEN "CAS:CONTACTOS" FOR INPUT AS
#1
60 FOR A=1 TO 26:FOR B=1 TO 26:INPUT
#1,T(A,B):T(A,B)=T(A,B)*100:NEXT B:NE
XT A
65 CLOSE #1
70 CLS
80 PRINT TAB(2);"ANALISIS DE LA REJIL
LA DE CARDANO"
85 PRINT TAB(2);"==================
============="
90 LOCATE 2,4:PRINT "TEXTO:";
100 INPUT T$
110 IF T$="0" THEN GOTO 9999
120 FOR I=1 TO LEN(T$)
130 IF I>LEN(T$) THEN GOTO 200
140 IF MID$(T$,I,1)>="A" AND MID$(T$,
I,1)<="Z" THEN GOTO 200
150 R$=""
160 IF I>1 THEN R$=LEFT$(T$,I-1)
170 IF I<LEN(T$) THEN R$=R$+RIGHT$(T$
,LEN(T$)-I)
180 T$=R$
190 GOTO 130
200 NEXT I
210 LT=LEN(T$)
220 IF LT=0 THEN GOTO 240
230 IF LT/36=INT(LT/36) THEN GOTO 260
235 T$=T$+"Z"
240 LT=LT+1
250 GOTO 230
260 LOCATE 2,4:PRINT SPACE$(255)
265 LOCATE 2,4:PRINT "TEXTO: ";T$
270 NB=INT(LT/36)
310 CA=ASC("A")-1
370 LOCATE 2,21:PRINT "PULSE CUALQUIE
R TECLA (C=IMPRIME)"
380 R$=INKEY$
390 IF R$="" THEN GOTO 380
395 IF R$="0" THEN GOTO 9999
430 CLS
440 FOR I=1 TO 6
450 FOR J=1 TO 6
460 G(J,I)=0
470 A(J,I)=0
480 NEXT J
490 NEXT I
510 LOCATE 14,2:PRINT "123456"
520 FOR I=1 TO 6
```

```
530 LOCATE 12,I+2:PRINT I
540 NEXT I
541 NH=0
545 R$=""
550 GOTO 700
560 LOCATE 5,21:PRINT "PULSE C,D,H,L,
R,P,T,N, o 0"
570 R$=INKEY$
580 IF R$="" THEN GOTO 570
590 LOCATE 0,21:PRINT TAB(31)
600 IF R$ <>"C" THEN GOTO 630
610 GOSUB 10000
620 GOTO 560
630 IF R$ <>"D" THEN GOTO 690
640 GOSUB 8000
650 G(Y,X)=0
660 LOCATE X+13,2+Y:PRINT " "
670 NH=NH-1
680 GOTO  560
690 IF R$ <> "H" THEN GOTO 740
700 GOSUB 8000
710 G(Y,X)=1
720 LOCATE 13+X,2+Y:PRINT CHR$(143)
725 NH=NH+1
730 GOTO 560
740 IF R$<>"L" AND R$<>"R" THEN GOTO
1105
745 GOSUB 8200
750 GOSUB 8000
753 XX=X
757 YY=Y
760 IF R$="L" THEN GOTO 830
770 X=X+1
780 IF X<=6 THEN GOTO 915
790 X=1
800 Y=Y+1
810 IF Y>6 THEN GOTO 1100
820 GOTO  915
830 X=X-1
840 IF X>=1 THEN GOTO 915
850 X=6
860 Y=Y-1
870 IF Y<1 GOTO 1100
915 P=0
917 FOR I=1 TO NB
920 FOR J=1 TO 2
960 IF R$="R" THEN P=P+T(ASC(MID$(T$,
(I-1)*36+(YY-1)*6+XX,1))-CA,ASC(MID$(
T$,(I-1)*36+(Y-1)*6+X,1))-CA)
970 X=7-X
980 Y=7-Y
990 XX=7-XX
1000 YY=7-YY
1010 R$=CHR$(ASC("R")+ASC("L")-ASC(R$
))
1020 NEXT J
1025 NEXT I
1030 IN=1
1040 FOR I=1 TO 4
1050 GOSUB 8100
1060 IF G(X,Y)=1 THEN IN=0
1070 NEXT I
1080 PRINT IN;X;",";Y;":";P,
1090 R$=INKEY$:IF R$="" THEN 1090
1095 IF R$<>"F" THEN GOTO 760
1100 CLS:GOTO 560
1105 IF R$="N" THEN GOTO 430
1110 IF R$<>"P" THEN GOTO 1200
1120 GOSUB 8200
1130 LOCATE 0,15:INPUT "LETRAS";L$
1140 IF LEN(L$)<>2 THEN GOTO 1130
1150 L1=ASC(MID$(L$,1,1))-CA
1160 L2=ASC(MID$(L$,2,1))-CA
1170 IF L1<1 OR L1>26 OR L2<1 OR L2>2
6 THEN GOTO 1130
1180 PRINT L$;":";T(L1,L2)
1190 GOTO 560
1200 IF R$<>"T" THEN GOTO 1460
1205 IF NH=9  THEN GOTO 1210
1207 PRINT "";:BEEP:BEEP:BEEP
1208 GOTO 560
1210 RF=1
1211 FOR Y=1 TO 6
1212 FOR X=1 TO 6
1213 A(Y,X)=G(Y,X)
1214 NEXT X
1215 NEXT Y
1219 FOR I=1 TO 4
1220 GOSUB 8200
1225 FOR J=1 TO NB
1230 FOR K=1 TO 4
1240 FOR Y=1 TO 6
1250 FOR X=1 TO 6
1260 IF A(Y,X)<>RF THEN GOTO 1270
1261 PRINT MID$(T$,(J-1)*36+(Y-1)*6+X
,1);
1262 A(Y,X)=0
1263 A(X,7-Y)=3-RF
1270 NEXT X
1280 NEXT Y
1290 RF=3-RF
1300 NEXT K
1310 NEXT J
1320 LOCATE 12,21:PRINT "PULSE "C,N,R
,S O 0"
1330 R$=INKEY$
1340 IF R$="" THEN GOTO 1330
1345 LOCATE 0,21:PRINT TAB(36)
1350 IF R$<>"C" THEN GOTO 1410
1360 GOSUB 10000
1370 GOTO 1320
1380 IF R$<>"N" THEN GOTO 1410
1381 FOR Y=1 TO 6
1382 FOR X=1 TO 6
1383 IF A(Y,X)<>RF THEN GOTO 1386
1384 A(Y,X)=0
1385 A(X,7-Y)=3-RF
1386 NEXT X
1387 NEXT Y
1388 RF=3-RF
1390 NEXT I
1400 GOTO 1219
```

```
1410 IF R$="R" THEN GOTO 560
1420 IF R$="F" OR R$="0" THEN GOTO 99
99
1430 LOCATE 0,21:PRINT "?":FOR T=1 TO
 10:BEEP:NEXT T:LOCATE 0,21:PRINT "?"
1450 GOTO 1320
1460 IF R$="0" THEN GOTO 9999
1490 GOTO 560
8000 LOCATE 0,15:INPUT "POSICION X,Y"
;X,Y
8005 IF X=0 OR Y=0 THEN GOTO 9999
8010 IF (X<1) OR (X>6) OR (X>INT(X))
OR (Y<1) OR (Y>6) OR (Y>INT(Y)) THEN
GOTO 8000
8020 IF R$="D" OR R$="L" OR R$="R" TH
EN GOTO 8080
8030 FOR I=1 TO 4
8040 GOSUB 8100
8050 IF G(Y,X)<>0 THEN GOTO 8090
8060 NEXT I
8070 RETURN
8080 IF G(Y,X)=1 THEN GOTO 8070
8090 PRINT "";:BEEP:BEEP:BEEP
8095 GOTO 8000
8100 S=Y
8110 Y=7-X
8120 X=S
8130 RETURN
8200 FOR I=10 TO 20
8210 LOCATE 0,I:PRINT TAB(36);" "
8220 NEXT I
8230 LOCATE 0,15
8240 RETURN
9999 END
10000 'RUTINA PARA LA IMPRESORA
10010 AA$=""
10020 A%=BASE(0)
10030 B%=BASE(0)
10040 OPEN "LPT:" AS #1
10050 FOR I%=A% TO A%+960
10060 C%=VPEEK(I%):AA$=AA$+CHR$(C%)
10070 IF LEN(AA$)=40 THEN PRINT #1,AA
$:AA$=""
10080 NEXT I%
10090 CLOSE #1
10100 RETURN
```

HILL

```
1 REM ********
2 REM *      *
3 REM * HILL *
4 REM *      *
5 REM ********
6 REM
10 SCREEN 0:KEY OFF:POKE -853,255:OUT
 170,255:CLEAR 2000
15 DATA 1,9,21,15,3,19,0,7,23,11,5,17
,25
20 PRINT TAB(5);"PROGRAMA DE CIFRADO
<HILL>"
25 PRINT TAB(5);STRING$(26,61)
30 LOCATE 2,2:PRINT "MODO: ";
40 M$=INPUT$(1)
50 IF M$="0" THEN 9999
60 IF M$<>"C" AND M$<>"D" THEN GOTO 3
0
90 LOCATE 2,2:PRINT "MODO: ";M$
100 LOCATE 2,4:PRINT "MATRIZ:";
110 INPUT A,B,C,D
120 LOCATE 0,5:PRINT SPC(255)
130 L=A*D-B*C
133 GOSUB 1000
137 DET=L
140 IF L<>0 THEN GOTO 180
150 LOCATE 6,16:PRINT "NO EXISTE MATR
IZ INVERSA":FOR T=1 TO 1000:NEXT T:LO
CATE 5,16:PRINT SPC(26)
160 LOCATE 9,4:PRINT SPC(9):LOCATE 9,
4
170 GOTO 100
180 IF L/2>INT(L/2)AND L/13>INT (L/13
) THEN GOTO 220
190 LOCATE 3,16:PRINT "EL DETERMINANT
E NO ES ADECUADO":FOR T=1 TO 1000:NEX
T T:LOCATE 3,16:PRINT SPC(30)
200 GOTO 100
220 LOCATE 2,6:PRINT "TEXTO: ";
230 INPUT T$
240 IF LEFT$(T$,1)="0" THEN GOTO 9999
260 FOR I=1 TO LEN(T$)
270 IF I>LEN(T$) THEN GOTO 330
275 T1$=MID$(T$,I,1)
280 IF T1$>="A" AND T1$<="Z" THEN GOT
O 330
290 R$=""
300 IF I>1 THEN R$=LEFT$(T$,I-1)
310 IF I<LEN(T$) THEN R$=R$+RIGHT$(T$
,LEN(T$)-I)
320 T$=R$
325 GOTO 270
330 NEXT I
340 LT=LEN(T$)
350 IF LT>1 THEN GOTO 380
360 LOCATE 0,6:PRINT "?":FOR T= TO 10
:BEEP:NEXT T:LOCATE 0,6:PRINT "?"
370 GOTO 220
380 IF LT/2=INT(LT/2) THEN GOTO 410
390 T$=T$+"Z"
```

```
400 LT=LT+1
410 LOCATE 2,6:PRINT "TEXTO: ";T$;SPC
(100)
415 CA=ASC("A")-1
416 DIM TN$(LT)
417 FOR N=1 TO LT
418 TN$(N)=MID$(T$,N,1)
419 NEXT N
420 IF M$="C" THEN GOTO 500
425 FOR I=1 TO 25 STEP 2
426 READ J
427 IF I=DET THEN R=J
428 NEXT I
430 I=A
433 A=D
437 D=I
440 B=-B
445 C=-C
450 L=A*R
453 GOSUB 1000
457 A=L
460 L=B*R
463 GOSUB 1000
464 B=L
465 L=C*R
466 GOSUB 1000
467 C=L
470 L=D*R
473 GOSUB 1000
477 D=L
480 PRINT
490 PRINT "MATRIZ INVERSA: ";A;",";B;
",";C;",";D
500 IF M$="D" THEN PRINT:PRINT "Texto
 descifrado: ";ELSE PRINT:PRINT "Text
o cifrado: ";
510 FOR I=1 TO LT STEP 2
520 L1=ASC(TN$(I))-CA
530 L2=ASC(TN$(I+1))-CA
540 L=A*L1+B*L2
550 GOSUB 1000
560 PRINT CHR$(LL+CA);
570 L=C*L1+D*L2
580 GOSUB 1000
590 PRINT CHR$(LL+CA);
600 NEXT I
610 GOTO  9999
1000 IF L>=0 AND L<26 GOTO 1040
1010 IF L<0 THEN L=L+26
1020 IF L>=26 THEN L=L-26
1030 GOTO 1000
1040 LL=L
1050 IF L=0 THEN LL=26
1060 RETURN
9999 END
```

GRONSFELD

```
1 REM *************
2 REM *           *
3 REM * GRONSFELD *
4 REM *           *
5 REM *************
6 REM
10 CLS:KEY OFF:POKE -853,255:OUT 170,
255
20 PRINT TAB(3);"PROGRAMA DE CIFRADO
<GRONSFELD>"
25 PRINT TAB(3);STRING$(31,61)
30 LOCATE 2,4:PRINT "MODO Y NUMERO CL
AVE";
40 INPUT M$
50 IF M$="0" THEN GOTO 9999
60 LM=LEN(M$)
70 IF LM<2 THEN GOTO 90
80 IF LEFT$(M$,1)="C" OR LEFT$(M$,1)=
"D" THEN GOTO 110
90 BEEP:LOCATE 9,15:PRINT "ENTRADA IN
VALIDA":FOR T=1 TO 500:NEXT T:LOCATE
9,15:PRINT SPC(18):LOCATE 24,4:PRINT
SPC(255)
100 CLEAR:GOTO 30
110 DIM K(LM-1)
120 FOR I=2 TO LM
130 K$=MID$(M$,I,1)
140 IF K$<"0" OR K$>"9" THEN GOTO 90
150 K(I-1)=VAL(K$)
160 NEXT I
170 LOCATE 2,4 :PRINT "MODO: ";LEFT$(
M$,1);" NUMERO CLAVE: ";MID$(M$,2)
180 LOCATE 2,6:PRINT"TEXTO:";
190 INPUT T$
200 IF T$="0" THEN GOTO 9999
210 LT=LEN(T$)
220 IF LT>0 THEN GOTO 250
240 GOTO 180
250 LOCATE 2,6:PRINT "TEXTO: ";T$
260 PRINT
263 CS=ASC(" ")
265 CA=ASC("A")
267 CZ=ASC("Z")
270 IF LEFT$(M$,1)="D" THEN GOTO 370
280 K=0
290 LOCATE 2,10:PRINT "Texto cifrado:
 ";:FOR I=1 TO LT
293 IF MID$(T$,I,1)><" " THEN GOTO 30
0
295 L=CS
```

```
297 GOTO 340
300 K=K+1
310 IF K=LM THEN K=1
320 L=ASC(MID$(T$,I,1))+K(K)
330 IF L>CZ THEN L=L-26
340 PRINT CHR$(L);
350 NEXT I
360 GOTO 9999
370 K=0
380 LOCATE 2,10:PRINT "Texto descifra
do: ";:FOR I=1 TO LT
383 IF MID$(T$,I,1)<>" " THEN GOTO 39
0
385 L=CS
387 GOTO 340
390 K=K+1
400 IF K=LM THEN K=1
410 L=ASC(MID$(T$,I,1))-K(K)
420 IF L<CA THEN L=L+26
430 PRINT CHR$(L);
440 NEXT I
9999 END
```

BIFIDO

```
1 REM **********
2 REM *        *
3 REM * BIFIDO *
4 REM *        *
5 REM **********
6 REM
10 CLS:SCREEN 0:KEY OFF:OUT 170,255:P
OKE -853,255
20 PRINT TAB(4);"PROGRAMA DE CIFRADO
<BIFIDO>"
25 PRINT TAB(4);STRING$(28,61)
30 LOCATE 1,3:PRINT "MODO Y PALABRA C
LAVE";
40 INPUT M$
50 IF M$="0" THEN GOTO 9999
60 IF LEN(M$)<2 THEN GOTO 80
70 IF LEFT$(M$,1)="C" OR LEFT$(M$,1)=
"D" THEN GOTO 100
80 LOCATE 1,3:PRINT SPC(255)
90 GOTO 30
100 DIM A(26)
110 DIM L(26)
115 CA=ASC("A")-1
120 A=0
130 FOR I=2 TO LEN(M$)
140 C=ASC(MID$(M$,I,1))-CA
150 IF L(C)>0 THEN GOTO 190
160 A=A+1
170 A(A)=C
180 L(C)=A
190 NEXT I
200 FOR I=1 TO 25
210 IF L(I)>0 THEN GOTO 250
220 A=A+1
230 A(A)=I
240 L(I)=A
250 NEXT I
255 LOCATE 0,3:PRINT SPC(255)
260 LOCATE 1,3:PRINT "MODO: ";LEFT$(M
$,1);"  CLAVE: ";MID$(M$,2,LEN(M$)-1)
270 LOCATE 1,5:PRINT "ALFABETO ALTERA
DO:";SPC(255)
280 FOR I=0 TO 4
290 FOR J=1 TO 5
300 LOCATE 20+J,5+I:PRINT CHR$(A(I*5+
J)+CA)
310 NEXT J
320 NEXT I
330 LOCATE 2,11:PRINT "LONGITUD DEL B
LOQUE";
340 INPUT B
345 IF B=0 THEN GOTO 9999
350 IF B>1 AND B=INT(B) THEN GOTO 380
360 LOCATE 0,11:PRINT SPC(36)
370 GOTO 330
380 LOCATE 2,11:PRINT "LONGITUD DEL B
LOQUE:";B
385 DIM B(2*B)
390 LOCATE 1,13:PRINT "TEXTO: ";
400 LINE INPUT T$
405 IF T$="0" THEN 9999
410 FOR I=1 TO LEN(T$)
420 IF I>LEN(T$) GOTO 490
430 IF MID$(T$,I,1)>="A" AND MID$(T$,
I,M1)<="Y" GOTO 490
440 R$=""
450 IF I>1 THEN R$=LEFT$(T$,I-1)
460 IF I<LEN(T$) THEN R$=R$+RIGHT$(T$
,LEN (T$)-I)
470 T$=R$
480 GOTO 420
490 NEXT I
500 LT=LEN(T$)
510 IF LT>1 THEN GOTO 540
520 LOCATE 0,13:PRINT "?":FOR T=1 TO
10:BEEP:NEXT T:LOCATE 0,13:PRINT " "
530 GOTO 390
540 FOR T=13 TO 21:PRINT TAB(36);:NEX
T T
545 LOCATE 0,13:PRINT "TEXTO: ";T$;SP
C(30)
550 IF LEFT$(M$,1)="D" THEN PRINT:PRI
NT "Texto descifrado: ";
560 IF LEFT$(M$,1)="D" THEN GOTO 720
```

```
570 PRINT:PRINT "Texto cifrado: ";:FO
R I=1 TO LT STEP B
580 T=B-1
590 IF I+T >LT THEN T=LT-I
600 FOR J=0 TO T
610 L=ASC(MID$(T$,I+J,1))-CA
620 A=L(L)
630 B(J+1)=INT((A-1)/5)+1
640 B(J+T+2)=A-5*(B(J+1)-1)
650 NEXT J
660 FOR J=0 TO 2*T STEP 2
670 C=(B(J+1)-1)*5+B(J+2)
680 PRINT CHR$(A(C)+CA);
690 NEXT J
700 NEXT I
710 GOTO 9999
720 FOR I=1 TO LT STEP B
730 T=B-1
740 IF I+T>LT THEN T=LT-I
750 FOR J=0 TO T
760 C=ASC(MID$(T$,I+J,1))-CA
770 A=L(C)
780 B(J*2+1)=INT((A-1)/5)+1
790 B(J*2+2)=A-5*(B(J*2+1)-1)
800 NEXT J
810 FOR J=0 TO T
820 L=(B(J+1)-1)*5+B(J+T+2)
830 PRINT CHR$(A(L)+CA);
840 NEXT J
850 NEXT I
9999 END
```

ANALISIS. ¿QUE CIFRADO?

```
1 REM ****************
2 REM *                  *
3 REM * QUE CIFRADO? *
4 REM *                  *
5 REM ****************
6 REM
10 CLEAR 1000:KEY OFF:POKE -853,255
15 SCREEN 0:OUT 170,255
20 PRINT TAB(1);"PROGRAMA DE ANALISIS
 <QUE CIFRADO?>"
25 PRINT TAB(1);STRING$(35,61)
30 LOCATE 1,4:PRINT "TEXTO: ";
40 INPUT T$
45 IF T$="0" THEN GOTO 9999
50 FOR I=1 TO LEN(T$)
60 IF I>LEN(T$) THEN GOTO 130
70 IF MID$(T$,I,1)>="A" AND MID$(T$,I
,1)<="Z" THEN GOTO 130
80 R$=""
90 IF I>1 THEN R$=LEFT$(T$,I-1)
100 IF I<LEN(T$) THEN R$=R$+MID$(T$,I
+1)
110 T$=R$
120 GOTO 60
130 NEXT I
140 LT=LEN(T$)
150 IF LT>25 THEN GOTO 180
160 LOCATE 9,15:PRINT "ENTRADA INCORR
ECTA":FOR T=1 TO 500:NEXT T:LOCATE 8,
15:PRINT SPC(20):LOCATE 10,2:PRINT SP
C(255)
170 GOTO 30
180 CA=ASC("A")-1
190 DIM F(27)
200 FOR I=1 TO LT
210 F(ASC(MID$(T$,I,1))-CA)=F(ASC(MID
$(T$,I,1))-CA)+1
220 NEXT I
230 M=0
240 OL=0
250 FOR I=1 TO 26
260 IF F(I)>M THEN M=F(I)
270 IF F(I)=0 THEN OL=1
280 NEXT I
290 CLS
310 SCREEN 2:PSET(45,170)
320 LINE-(255,170)
325 LINE(255,0)-(255,170)
330 LINE(45,170)-(45,0)
335 FOR W=0 TO 170 STEP 8.5:LINE(255,
W)-(45,W),15:NEXT W
336 FOR Q=0 TO 170 STEP 42.5:LINE(40,
Q)-(45,Q):NEXT Q
340 OPEN"GRP:"FOR OUTPUT AS #1
341 PSET(15,0),0:PRINT#1,"20%"
342 PSET(15,37),0:PRINT#1,"15%"
343 PSET(15,80),0:PRINT#1,"10%"
344 PSET(15,122),0:PRINT#1," 5%"
345 PSET(15,165),0:PRINT#1," 0%"
347 PSET(48,175),0:PRINT#1,"abcdefghi
jklmnopqrstuvwxyz"
349 X=40:H=F(1):IF H>.2 THEN H=.2
370 FOR I=1 TO 26
373 H=F(I)/LT
377 IF H>.2 THEN H=.2
379 X=X+8
380 FOR T=1 TO 4:LINE(X+T,170)-(X+T,1
70-H*850):NEXT T
390 NEXT I
400 IF INKEY$="" THEN GOTO 400
410 CLS
420 S=0
430 FOR I=1 TO 26
440 S=S+F(I)*(F(I)-1)
```

```
450 NEXT I
460 IC=S/(LT*(LT-1))
470 SCREEN 0:LOCATE 1,2:PRINT "PROGRA
MA DE ANALISIS <QUE CIFRADO?>":PRINT
TAB(1);STRING$(35,45):LOCATE 2,6:PRIN
T "INDICE DE COINCIDENCIA DE LETRAS":
PRINT TAB(2);"AISLADAS:";IC
480 DIM P(702)
490 LL=LT
500 IF LL/2 >INT(LL/2)THEN LL=LL-1
510 FOR I=1 TO LL STEP 2
520 P=(ASC(MID$(T$,I,1))-CA)*26+ASC(M
ID$(T$,I+1,1))-CA
530 P(P)=P(P)+1
540 NEXT I
550 S=0
560 FOR I=1 TO 676
570 S=S+P(I)*(P(I)-1)
580 NEXT I
590 IP=S/(LL*(LL-1))
600 LOCATE 0,8:PRINT STRING$(37,45):P
RINT TAB(2);"INDICE DE COINCIDENCIA D
E PARES DE   LETRAS:";IP:PRINT STRING
$(37,32)
9999 END
```

ANALISIS GRONSFELD

```
1 REM **********************
2 REM *                        *
3 REM * ANALISIS GRONSFELD *
4 REM *                        *
5 REM **********************
6 REM
10 KEYOFF:CLS
15 DIM E(26),T(26,26),C(26),W(20),O(2
5),P(25,10),K(25)
20 DIM F$(255),D(255)
30 LOCATE 3,9:PRINT "INTRODUZCA UNA C
INTA CON DATOS":PRINT TAB(7);"Y LUEGO
 PULSE UNA TECLA"
40 A$=INKEY$:IF A$="" THEN GOTO 40
41 GOTO 70
45 OPEN "CAS:FRECUENCIAS" FOR INPUT A
S #1
50 FOR A=1 TO 26:INPUT #1,E(A):E(A)=E
(A)*100:NEXT A:CLOSE #1
55 OPEN "CAS:CONTACTOS" FOR INPUT AS#
1
60 FOR A=1 TO 26:FOR B=1 TO 26:INPUT
#1,T(A,B):T(A,B)=T(A,B)*100:NEXT B:NE
XT A:CLOSE #1
70 CLS
80 PRINT TAB(3);"PROGRAMA DE ANALISIS
 <GRONSFELD>"
90 PRINT TAB(3);STRING$(32,61)
100 LOCATE 2,4:INPUT "TEXTO:";T$
105 IF LEFT$(T$,1)="0" THEN GOTO 9999
110 FOR I=1 TO LEN(T$)
120 IF I>LEN(T$) THEN GOTO 190
125 T1$=MID$(T$,I,1)
130 IF T1$>="A" AND T1$<="Z" THEN GOT
O 190
140 R$=""
150 IF I>1 THEN R$=LEFT$(T$,I-1)
160 IF I<LEN(T$) THEN R$=R$+RIGHT$(T$
,LEN(T$)-I)
170 T$=R$
180 GOTO 120
190 NEXT I
210 LT=LEN(T$)
220 IF LT>10 THEN GOTO 250
230 LOCATE 13,19:PRINT "TEXTO CORTO":
FOR T=1 TO 10:BEEP:NEXT T:LOCATE 13,1
9:PRINT SPC(11):LOCATE 10,4:PRINT SPC
(10)
240 GOTO 100
250 LOCATE 0,15:PRINT "TEXTO:";T$
255 CA=ASC("A")-1
260 FOR QW=1 TO LT:F$(QW)=" ":D(QW)=1
:NEXT QW
280 NR=0
290 CLS
295 PRINT "FACTORES DE REPETICION:"
300 GOSUB 5000
430 PRINT "HAY";NR;"REPETICION";:IF N
R>1 THEN PRINT "ES" ELSE PRINT
740 FOR I=1 TO LT
750 L=ASC(MID$(T$,I,1))-CA
760 C(L)=C(L)+1
770 NEXT I
780 S=0
790 FOR I=1 TO 26
800 S=S+C(I)*(C(I)-1)
810 NEXT I
820 IC=S/(LT*(LT-1))
830 PRINT "INDICE DE COINCIDENCIA:";I
C
840 INPUT "LONGITUD DE LA CLAVE A BUS
CAR";KL
850 IF KL=0 THEN GOTO 9999
860 IF KL<2 OR KL>LT/2 OR KL>INT(KL)
THEN GOTO 840
920 PRINT "LONGITUD DE LA CLAVE:";KL
930 FOR QW=1 TO 25:K(QW)=0:FOR WQ=1 T
O 10:P(QW,WQ)=0:NEXT WQ:NEXT QW
931 FOR QW=1 TO LT:F$(QW)=" ":NEXT QW
935 FOR I=1 TO KL:K(I)=-1:NEXT I
940 FOR I=1 TO 26
950 C(I)=C(I)/LT
```

```
960 NEXT I
961 PRINT TAB(11);"PULSE UNA TECLA"
962 A$=INKEY$:IF A$="" THEN GOTO 962
965 CLS
969 GOTO 7000
970 FOR C=1 TO KL
980 GOSUB 8000
990 NEXT C
1140 NC=0
1150 NC=NC+1
1160 IF LT/(NC*KL)>15 THEN GOTO 1150
1165 CL=NC*KL
1167 NR=LT/CL
1260 GOSUB 8200
1270 LOCATE 3,20:PRINT "PULSE A,B,C,D
,E,F,K,N,P,S,T,W o 0"
1280 R$=INKEY$
1290 IF R$="" THEN GOTO 1280
1300 IF R$="A" THEN GOTO 7000
1310 IF R$<>"B" THEN GOTO 1380
1320 GOSUB 8300
1330 K(C)=-1
1333 FOR I=1 TO 10
1335 P(C,I)=0
1337 NEXT I
1340 FOR I=C TO LT STEP KL
1350 F$(I)=" "
1360 NEXT I
1370 GOTO 1260
1380 IF R$<>"C" THEN GOTO 1410
1390 GOSUB 10020
1400 GOTO 1270
1410 IF R$<>"D" THEN GOTO 1450
1420 FOR QW=1 TO LT:F$(QW)=" ":NEXT Q
W
1430 FOR I=1 TO KL
1431 K(I)=-1
1432 NEXT I
1435 FOR QW=1 TO 25:FOR WQ=1 TO 10:P(
QW,WQ)=0:NEXT WQ:NEXT QW
1440 GOTO 1260
1450 IF R$<>"E" THEN GOTO 1500
1460 GOSUB 9000:PRINT "LETRA";:L$=INP
UT$(1)
1465 IF L$="0" THEN GOTO 9999
1470 IF L$<"A" OR L$>"Z" THEN GOTO 14
60
1480 PRINT L$;":";E(ASC(L$)-CA)
1490 GOTO 1270
1500 IF R$<>"F" THEN GOTO 1550
1505 Z=2
1510 FOR C=1 TO KL
1520 IF K(C)<0 THEN IF (F$(KL+C-1)<>"
 ") OR (F$(C+1)<>" ") THEN GOSUB 8000
:GOSUB 8200
1530 NEXT C
1533 Z=Z-1
1536 IF Z>=0 THEN GOTO 1510
1537 FOR I=1 TO KL
1538 IF K(I)<0 THEN GOTO 1505
1539 NEXT I
1540 GOTO 1260
1550 IF R$<>"K" THEN GOTO 1580
1560 CLS
1570 GOTO 840
1580 IF R$<>"N" THEN GOTO 1620
1590 GOSUB 8300
1600 GOSUB 8000
1610 GOTO 1260
1620 IF R$="P" THEN GOTO 7230
1625 IF R$<>"S" THEN GOTO 1660
1630 CLS
1631 GOSUB 9000:PRINT "CLAVE:";
1632 FOR I=1 TO KL
1633 PRINT K(I);
1634 NEXT I
1640 PRINT:PRINT:FOR I=1 TO LT:PRINT
F$(I);:NEXT I:PRINT
1650 GOTO 9999
1660 IF R$<>"T" THEN GOTO 1740
1665 GOSUB 9000
1670 PRINT "LETRAS:";:L$=INPUT$(2)
1675 IF L$="0" THEN GOTO 9999
1690 L1=ASC(LEFT$(L$,1))-CA
1700 L2=ASC(RIGHT$(L$,1))-CA
1710 IF L1<1 OR L1>26 OR L2<1 OR L2>2
6 THEN GOTO 1665
1715 LOCATE 20,21
1720 PRINT L$;":";T(L1,L2)
1730 GOTO 1270
1740 IF R$<>"W" THEN GOTO 1800
1750 GOSUB 8300
1755 GOSUB 9000
1760 INPUT "CLAVE";D
1770 IF D<0 OR D>9 OR D>INT(D) THEN G
OTO 1760
1780 GOSUB 8170
1790 GOTO 1260
1800 IF R$="0" THEN GOTO 9999
1805 LOCATE 33,21
1810 PRINT "?":FOR T=1 TO 10:BEEP:NEX
T T:LOCATE 33,21:PRINT " "
1820 GOTO 1270
5000 FOR I=2 TO 6
5010 FOR K=1 TO LT-2*I+1
5020 FOR J=I+K TO LT-I+1
5030 IF MID$(T$,K,I)=MID$(T$,J,I) THE
N GOSUB 6000
5040 NEXT J:NEXT K:NEXT I
5050 RETURN
6000 D=J-K
6005 NR=NR+1
6010 PRINT STR$(NR);".";STR$(K);",";J
;MID$(T$,K,I);" DIST=";D;"DIV";
6030 W=D:IF D>10 THEN W=10
6040 FOR DI=2 TO W
6050 IF D/DI=INT(D/DI) THEN PRINT "-"
;DI;
6060 NEXT DI
6070 PRINT:RETURN
7000 GOSUB 9000:INPUT "PALABRA PROBAB
LE: ";W$
```

```
7010 IF W$="0" THEN GOTO 9999
7020 IF W$="" THEN GOTO 970
7030 LW=LEN(W$)
7040 FOR QW=1 TO 25:O(QW)=0:NEXT QW
7050 FOR I=1 TO LW
7060 W(I)=ASC(MID$(W$,I,1))-CA
7065 IF W(I)<1 OR W(I)>26 THEN GOTO 7
000
7070 NEXT I
7080 NP=0
7100 FOR I=0 TO LT-LW-1
7110 FOR J=1 TO LW
7120 L=ASC(MID$(T$,I+J,1))-CA
7130 FOR K=0 TO 9
7140 N=L-K
7150 IF N<1 THEN N=N+26
7160 IF N=W(J) THEN GOTO 7190
7170 NEXT K
7180 GOTO 7220
7190 NEXT J
7200 NP=NP+1
7210 O(NP)=I+1
7220 NEXT I
7230 CLS
7235 IF NP>0 THEN GOTO 7260
7240 PRINT "<";W$; "> NO PUEDE SER"
7250 GOTO 7000
7260 PRINT "PUEDE ESTAR EN";NP;"SITIO
";:IF NP>1 THEN PRINT "S" ELSE PRINT
7270 FOR I=1 TO NP
7280 PRINT I;". CARACTER ";O(I);"-";
7290 PRINT MID$(T$,O(I),LW)
7330 NEXT I
7335 PRINT
7340 INPUT "NUMERO DE OPCION:";O
7345 IF O=0 THEN GOTO 9999
7350 IF O<1 OR O>NP OR O>INT(O) THEN
GOTO 7340
7360 P=O(O)
7370 C=P-KL*INT(P/KL)
7380 IF C=0 THEN C=KL
7390 FOR J=0 TO LW-1
7400 L=ASC(MID$(T$,P+J,1))-CA
7410 FOR K=0 TO 9
7420 N=L-K
7430 IF N<1 THEN N=N+26
7440 IF N<>W(J+1) THEN NEXT K
7450 D=K
7455 GOSUB 8170
7460 C=C+1
7470 IF C>KL THEN C=C-KL
7480 NEXT J
7490 CLS
7500 GOTO 1140
8000 B=999
8010 D=0
8020 FOR K=0 TO 9
8025 IF P(C,K+1)<>0 THEN GOTO 8160
8030 T=0
8040 N=L-K
8050 IF N<1 THEN N=N+26
8060 T=T+(LT/KL)*ABS(E(N)-C(L))
8065 FOR J=0 TO LT-KL STEP KL
8070 P=C+J
8080 L=ASC(MID$(T$,P,1))-CA
8100 IF P>1 AND F$(P+1)<>" " THEN T=T
-T(ASC(F$(P-1))-CA,N)
8110 IF P<L AND F$(P+1)<>" " THEN T=T
-T(N,ASC(F$(P+1))-CA)
8120 NEXT J
8130 IF T>B THEN GOTO 8160
8140 B=T
8150 D=K
8160 NEXT K
8170 K(C)=D
8175 P(C,D+1)=1
8180 FOR I=C TO LT STEP KL
8182 L=ASC(MID$(T$,I,1))-CA-D
8184 IF L<1 THEN L=L+26
8186 F$(I)=CHR$(L+CA)
8188 NEXT I
8190 RETURN
8200 LOCATE 7,1:FOR I=1 TO KL:PRINT R
IGHT$(STR$(I),1);:NEXT I
8201 LOCATE 7,4
8205 FOR I=0 TO NR-1
8210 PRINT TAB(7);
8211 FOR QW=CL*I+1 TO CL*(I+1):PRINT
F$(QW);:NEXT QW:PRINT
8220 NEXT I
8225 IF LT/CL>INT(LT/CL) THEN LOCATE
7,I+4:FOR QW=CL*I+1 TO LT:PRINT F$(QW
);:NEXT QW:PRINT
8226 LOCATE 1,2
8236 PRINT "CLAVE=";
8240 FOR J=1 TO KL
8250 PRINT MID$(STR$(K(J)),2,1);
8260 NEXT J
8262 PRINT FF$
8265 PRINT
8280 RETURN
8300 GOSUB 9000:INPUT "QUE COLUMNA";C
8310 IF C=0 THEN GOTO 9999
8320 IF C<1 OR C>KL OR C>INT(C) THEN
GOTO 8300
8330 RETURN
9000 LOCATE 0,20:PRINT SPC(74):LOCATE
 0,20:RETURN
9999 END
10000 REM ************************
10010 REM RUTINA PARA LA IMPRESORA
10020 ZZ$=""
10030 A%=BASE(0)
10040 B%=BASE(2)
10050 OPEN "LPT:" AS #1
10060 FOR I%=A% TO A%+960
10070 C%=VPEEK(I%):ZZ$=ZZ$+CHR$(C%)
10080 IF LEN(ZZ$)=40 THEN PRINT #1,ZZ
$:ZZ$=""
10090 NEXT I%
10100 CLOSE #1
10110 RETURN
```

SEGURO

```
1 REM **********
2 REM *          *
3 REM * SEGURO *
4 REM *          *
5 REM **********
6 REM
10 KEY OFF:POKE -853,255:OUT 170,255
15 CLEAR 1000:CLS
20 PRINT TAB(4);"PROGRAMA DE CIFRADO
<SEGURO>"
25 PRINT TAB(4);STRING$(28,61)
30 LOCATE 2,4:PRINT "MODO:";
40 M$=INPUT$(1)
50 IF M$="0" GOTO 9999
60 IF M$="C" OR M$="D" THEN GOTO 90
70 LOCATE 7,4:PRINT SPC(255)
80 GOTO 30
90 LOCATE 2,2:PRINT "MODO:";M$
100 LOCATE 2,4:PRINT "NUMERO CLAVE:";
110 INPUT K
120 IF K=0 THEN GOTO 9999
130 IF K>0 AND K<65536! AND K=INT(K)
THEN GOTO 160
140 LOCATE 0,4:PRINT "?":FOR T=1 TO 1
0:BEEP:NEXT T:LOCATE 0,4:PRINT " "
150 GOTO 100
160 LOCATE 2,4:PRINT "NUMERO CLAVE:";
K
170 LOCATE 2,6:PRINT "PALABRA CLAVE:"
;
180 INPUT K$
190 IF K$="0" THEN GOTO 9999
200 LK=LEN(K$)
210 IF LK>0 THEN GOTO 240
220 LOCATE 17,6:PRINT SPC(255)
230 GOTO 170
240 DIM A(25)
250 DIM L(25)
260 CA=ASC("A")-1
270 A=0
280 FOR I=1 TO LK
285 KM$=MID$(K$,I,1)
290 C=ASC(KM$)-CA
300 IF C<1 OR C>25 THEN GOTO 220
310 IF L(C)>0 THEN GOTO 350
320 A=A+1
330 A(A)=C
340 L(C)=A
350 NEXT I
360 FOR I=1 TO 25
370 IF L(I)>0 THEN GOTO 410
380 A=A+1
390 A(A)=I
400 L(I)=A
410 NEXT I
420 LOCATE 2,6:PRINT "ALFABETO ALTERA
DO";SPC(20)
430 FOR I=0 TO 4
440 FOR J=1 TO 5
450 LOCATE 20+J,6+I:PRINT CHR$(A(I*5+
J)+CA)
460 NEXT J
470 NEXT I
480 LOCATE 2,12:PRINT "TEXTO:";
490 INPUT T$
500 IF T$="0" THEN GOTO 9999
510 FOR I=1 TO LEN(T$)
520 IF I>LEN(T$) THEN GOTO 590
530 T1$=MID$(T$,I,1)
535 IF T1$>="A" AND T1$<="Z" THEN GOT
O 590
540 R$=""
550 IF I>1 THEN R$=LEFT$(T$,I-1)
560 IF I<LEN(T$) THEN R$=R$+RIGHT$(T$
,LEN(T$)-I)
570 T$=R$
580 GOTO 520
590 NEXT I
600 LT=LEN(T$)
610 IF LT>0 THEN GOTO 640
620 LOCATE 0,12:PRINT "?"
630 GOTO 480
640 LOCATE 2,12:PRINT "TEXTO: ";T$;SP
C(200);STRING$(199,8)
646 IF M$="C" THEN PRINT:PRINT "Texto
 cifrado: ";
647 IF M$="D" THEN PRINT:PRINT "Texto
 descifrado: ";
648 DIM TM$(LT)
649 W=RND(-K):W=0
650 FOR M=1 TO LT
651 TM$(M)=MID$(T$,M,1)
652 NEXT M
660 IF M$="D" THEN GOTO 760
670 FOR I=1 TO LT
680 C=ASC(TM$(I))-CA
690 X=INT((C-1)/5)+INT(5*RND(1))+2
700 IF X>5 THEN X=X-5
710 Y=C-INT((C-1)/5)*5+INT(5*RND(1))+
1
720 IF Y>5 THEN Y=Y-5
730 PRINT CHR$(L((X-1)*5+Y)+CA);
740 NEXT I
750 GOTO 9999
760 FOR I=1 TO LT
770 C=A(ASC(TM$(I))-CA)
780 X=INT((C-1)/5)-INT(5*RND(1))
790 IF X<1 THEN X=X+5
800 Y=C-INT((C-1)/5)*5-INT(5*RND(1))-
1
810 IF Y<1 THEN Y=Y+5
820 PRINT CHR$((X-1)*5+Y+CA);
830 NEXT I
9999 END
```

CREACION DE DATOS

```
1 REM **********************
2 REM *                      *
3 REM *     PROGRAMA DE      *
4 REM * CREACION DE DATOS *
5 REM *                      *
6 REM **********************
7 REM
10 DIM E(26),T(26,26)
20 CLS
30 LOCATE 0,0:PRINT "INTRODUCE LA FRE
CUENCIA DE CADA LETRA";:PRINT TAB(4)
"A MEDIDA QUE VAYAN APARECIENDO"
40 FOR I=1 TO 26
50 LOCATE 16,3:PRINT CHR$(64+I);:INPU
T E(I):LOCATE 16,3:PRINT SPC(20)
60 NEXT I
70 LOCATE 0,5:PRINT "AHORA INTRODUCE
LOS CONTACTOS POR EL":PRINT TAB(2);"L
ADO DERECHO PARA CADA UNO DE LOS":PRI
NT TAB(5);"SIGUIENTES PARES DE LETRAS
:"
80 FOR I=1 TO 26
90 FOR J=1 TO 26
100 LOCATE 16,9:PRINT CHR$(64+I);CHR$
(64+J);:INPUT T(I,J):LOCATE 16,9:PRIN
T SPC(20)
110 NEXT J
120 NEXT I
130 LOCATE 0,12:PRINT TAB(1);"PREPARA
 LA CINTA PARA ALMACENAR LOS":PRINT T
AB(1);"DATOS Y LUEGO PULSA CUALQUIER
TECLA"
140 A$=INKEY$:IF A$="" THEN GOTO 140
150 OPEN "CAS:CONTACTOS" FOR OUTPUT A
S #1
160 FOR I=1 TO 26:PRINT #1,E(I):NEXT
I
170 CLOSE #1
180 OPEN "CAS:FRECUENCIAS" FOR OUTPUT
 AS #1
190 FOR I=1 TO 26:FOR J=1 TO 26:PRINT
 #1,T(I,J):NEXT J:NEXT I
200 CLOSE #1
210 FOR T=1 TO 21:PRINT:BEEP:NEXT T:P
RINT TAB(6);"LOS DATOS ESTAN SALVADOS
"
220 END
```

Programas para Amstrad

CESAR

```
10 REM CESAR
20 MODE 1
30 CLS
40 PRINT "PROGRAMA DE CIFRADO 'CESAR'"
50 LOCATE 3,3
60 INPUT "MODO Y CLAVE";m$
70 IF LEFT$(m$,1)="0" THEN GOTO 9999

80 IF LEFT$(m$,1)<"c" OR LEFT$(m$,1)>"d"
THEN 110
90 IF MID$(m$,2,1)<"a" OR MID$(m$,2,1)>"
z" THEN 110
100 GOTO 140
110 LOCATE 2,3:PRINT "? ";
130 GOTO 60
140 LOCATE 1,3:PRINT  " MODO : ";LEFT$(m
$,1);" CLAVE : ";MID$(m$,2,1)
150 k=ASC(MID$(m$,2,1))-ASC("a")
160 LOCATE 1,5
170 INPUT "TEXTO :";t$
180 IF LEFT$(t$,1)="0" THEN 9999
190 IF LEFT$(m$,1)="c" THEN 210
200 k=-k
210 l=LEN(t$)
230 PRINT:FOR i=1 TO l
240 c$=MID$(t$,i,1)
250 IF "a"<=c$ AND c$<="z" THEN 280
260 PRINT " ";
270 GOTO 310
280 w=ASC(c$)-ASC("a")+k
290 GOSUB 450
300 PRINT CHR$(w+ASC("a"));
310 NEXT i
320 IF LEFT$(m$,1)="c" THEN  9999
330 LOCATE 3,25
340 PRINT "Pulse 's' para seguir,'n' par
a detenerse"
350 r$=INKEY$
360 IF r$="" THEN  350
370 IF r$="n" THEN  9999
380 IF r$="s" THEN  410
390 LOCATE 1,25:PRINT "? ";
400 GOTO 340
410 CLS:LOCATE 1,2:w=1-k
420 GOSUB 450
430 k=-w
440 GOTO 230
450 IF w<=25 THEN  480
460 w=w-26
470 GOTO 500
480 IF w>=0 THEN  500
490 w=w+26
500 RETURN
9999 REM fin
```

MONO

```
10 REM CIFRADO MONOALFABETICO
15 MODE 1
16 CLS
20 PRINT "PROGRAMA DE CIFRADO MONOALFABE
TICO"
30 LOCATE 3,3
40 PRINT "MODO,MEZCLA Y CLAVE:";
50 INPUT m$
60 IF m$="0" THEN 9999
70 l=LEN(m$)
80 IF l<3 OR l>28 THEN 150
90 IF LEFT$(m$,1)<"c" OR LEFT$(m$,1)>"d"
 THEN 150
100 IF MID$(m$,2,1)<"s" OR MID$(m$,2,1)>
"t" THEN 150
110 FOR i=3 TO l
120 IF MID$(m$,i,1)<"a" OR MID$(m$,i,1)>
"z" THEN 150
130 NEXT i
131 CLS
132 LOCATE 1,3:PRINT "MODO = ";LEFT$(m$,
1);
134 PRINT " MEZCLA = ";MID$(m$,2,1);"
          "
136 LOCATE 1,5:PRINT "CLAVE : "; MID$(m$
,3,l)
140 GOTO 220
150 LOCATE 1,5
160 IF l>28 THEN 190
170 PRINT m$
180 GOTO 200
190 PRINT LEFT$(m$,28)
200 LOCATE 1,3:PRINT "?";
210 GOTO 16
220 m$=m$+"abcdefghijklmnopqrstuvwxyz"
230 la=LEN(m$)
240 c$=""
250 ca=ASC("a")-1
260 DIM a$(27):FOR k=0 TO 26:a$(k)=" ":N
EXT k
270 FOR i=3 TO la
280 as=ASC(MID$(m$,i,1))-ca
290 IF a$(as)<>" " THEN 310
300 c$=c$+MID$(m$,i,1)
310 IF i<>1 THEN 330
320 b=LEN(c$)
330 a$(as)="*"
340 NEXT i
350 IF MID$(m$,2,1)="s" THEN 600
360 d=INT(26/b)
362 IF b*d=26 THEN 365
364 d=d+1
365 lc=b*d
390 IF lc<=26 THEN 430
400 FOR i=27 TO lc
410 c$=c$+"*"
420 NEXT i
425 ERASE a$
430 DIM a$(d,b)
435 w=1
440 FOR j=1 TO d
450 FOR i=1 TO b
460 a$(j,i)=MID$(c$,w,1)
465 w=w+1
470 NEXT i
480 NEXT j
490 c$=""
500 FOR i=1 TO b
510 FOR j=d TO 1 STEP -1
520 IF a$(j,i)="*" THEN 540
530 c$=c$+a$(j,i)
540 NEXT j
550 NEXT i
600 LOCATE 1,7:PRINT "TEXTO :";
610 INPUT t$
620 LOCATE 1,12:PRINT "       "
630 IF t$="0" THEN 9999
640 lt=LEN(t$)
650 IF LEFT$(m$,1)="c" THEN 730
660 DIM p$(26)
670 FOR i=1 TO 26
680 p$(ASC(MID$(c$,i,1))-ca)=CHR$(ca+i)
690 NEXT i
700 FOR i=1 TO 26
710 MID$(c$,i,1)=p$(i)
720 NEXT i
725 LOCATE 1,13
730 FOR i=1 TO lt
740 IF MID$(t$,i,1)<"a" OR MID$(t$,i,1)>
"z" THEN 770
750 PRINT MID$(c$,ASC(MID$(t$,i,1))-ca,1
);
760 GOTO 780
770 PRINT " ";
780 NEXT i
9999 REM fin
```

PROGRAMA DE ANALISIS DE FRECUENCIAS

```
10 REM ANALISIS DE FRECUENCIAS
12 DIM e(26),d(26),t(26,26),f(26,26)
15 MODE 1
16 CLS
20 PRINT "PROGRAMA DE ANALISIS DE FRECUE
NCIAS"
30 LOCATE 3,3:PRINT "TEXTO";
40 INPUT t$
50 IF t$="0" THEN 9999
60 FOR i=1 TO LEN(t$)
70 IF i>LEN(t$) THEN 140
80 IF MID$(t$,i,1)>="a" AND MID$(t$,i,1)
<="z" THEN 140
90 r$=""
100 IF i>1 THEN r$=MID$(t$,1,i-1)
110 IF i<LEN(t$) THEN r$=r$+MID$(t$,i+1,
LEN(t$))
120 t$=r$
130 GOTO 70
140 NEXT i
150 lt=LEN(t$)
160 IF lt>3 THEN 190
170 LOCATE 1,3:PRINT "?"
180 GOTO 30
190 CLS:LOCATE 1,1::PRINT "TEXTO: ";t$
200 GOSUB 8000
210 ca=ASC("a")-1
230 PRINT "FRECUENCIA RELATIVA DE LAS LE
TRAS:":PRINT:PRINT
240 FOR i=1 TO lt
250 e(ASC(MID$(t$,i,1))-ca)=e(ASC(MID$(t
$,i,1))-ca)+1
260 NEXT i
270 FOR i=1 TO 26
275 IF i>=14 THEN LOCATE 19,i-10
280 PAPER 5:PEN 4:PRINT CHR$(i+ca);
285 PAPER 0:PEN 1:PRINT ":";e(i)/lt*100;
:PRINT CHR$(6)
290 NEXT i
300 GOSUB 8000
310 PRINT TAB(10);"LETRAS REPETIDAS:"
320 FOR i=1 TO lt-1
330 IF MID$(t$,i,1)=MID$(t$,i+1,1) THEN
d(ASC(MID$(t$,i,1))-ca)=d(ASC(MID$(t$,i,
1))-ca)+1
340 NEXT i
350 LOCATE 1,4:PRINT "LETRAS REPETIDAS:"
:PRINT:PRINT
360 FOR i=1 TO 26
365 IF i>=14 THEN LOCATE 19,i-7
370 PAPER 5:PEN 4:PRINT CHR$(i+ca);
375 PAPER 0:PEN 1:PRINT ":";d(i);CHR$(6)
380 NEXT i
390 GOSUB 8000
400 PRINT "FRECUENCIAS DE DOS LETRAS CON
SECUTIVAS:":PRINT
420 FOR i=1 TO lt-1
430 t(ASC(MID$(t$,i,1))-ca,ASC(MID$(t$,i
+1,1))-ca)=t(ASC(MID$(t$,i,1))-ca,ASC(MI
D$(t$,i+1,1))-ca)+1
440 NEXT i
450 FOR i=1 TO 26
460 FOR j=1 TO 26
470 IF t(i,j)>0 THEN PAPER 5:PEN 4:PRINT
 CHR$(i+ca);CHR$(j+ca);:PAPER 0:PEN 1:PR
INT ": ";t(i,j);CHR$(6):cc=cc+1
480 IF VPOS(#0)=20 AND POS(#0)<16 THEN G
OSUB 8000
490 NEXT j
500 NEXT i
510 GOSUB 8000
520 PRINT "LETRAS EN ORDEN INVERSO:":PRI
NT:PRINT
530 FOR i=1 TO 26
540 FOR j=1 TO 26
550 IF t(i,j)>0 AND t(j,i)>0 AND i<>j AN
D f(i,j)=0 AND f(j,i)=0 THEN PAPER 5:PEN
 4:PRINT CHR$(i+ca);CHR$(j+ca);:PAPER 0:
PEN 1:PRINT ":";t(i,j);"     ";:PAPER 5:P
EN 4:PRINT CHR$(j+ca);CHR$(i+ca);:PAPER
0:PEN 1:PRINT ":";t(j,i):f(i,j)=1
560 IF VPOS(#0)=20 AND POS(#0)<16 THEN G
OSUB 8000
570 NEXT j
580 NEXT i
590 GOSUB 8000
595 PRINT "PROBABILIDAD LADO DERECHO:":P
RINT
610 FOR i=1 TO 26
620 IF e(i)=0 THEN 660
630 FOR j=1 TO 26
640 f(i,j)=t(i,j)/e(i)
650 NEXT j
660 NEXT i
680 FOR i=1 TO 26
690 FOR j=1 TO 26
700 IF f(i,j)>0 THEN PAPER 5:PEN 4:PRINT
 CHR$(i+ca);CHR$(j+ca);:PAPER 0:PEN 1:PR
INT ": ";f(i,j)*100;CHR$(6)
710 IF VPOS(#0)=20 AND POS(#0)<16 THEN G
OSUB 8000
720 NEXT j
730 NEXT i
740 GOSUB 8000
750 PRINT "PROBABILIDAD DE CONTACTO LADO
 IZQUIERDO:":PRINT
760 FOR i=1 TO 26
770 IF e(i)=0 THEN 810
780 FOR j=1 TO 26
790 f(i,j)=t(j,i)/e(i)
800 NEXT j
810 NEXT i
830 FOR i=1 TO 26
840 FOR j=1 TO 26
850 IF f(i,j)>0 THEN PAPER 5:PEN 4:PRINT
 CHR$(j+ca);CHR$(i+ca);:PAPER 0:PEN 1:PR
```

```
INT ": ";f(i,j)*100;CHR$(6)
860 IF VPOS(#0)=20 AND POS(#0)<16 THEN G
OSUB 8000
870 NEXT j
880 NEXT i
890 GOSUB 8000
895 PRINT TAB(13);"TRIGRAMAS":PRINT:PRIN
T
900 DIM g(26,lt)
910 FOR i=1 TO 26
920 FOR j=2 TO lt-1
930 IF MID$(t$,j,1)=CHR$(i+ca) THEN g(i,
j)=1
940 NEXT j
950 NEXT i
960 PRINT "GRUPOS DE TRES LETRAS CONSECU
TIVAS:":PRINT
970 FOR i=1 TO 26
980 IF e(i)=0 OR (e(i)=1 AND (MID$(t$,1,
1)=CHR$(i+ca) OR MID$(t$,lt,1)=CHR$(i+ca
))) THEN 1050
990 PAPER 5:PEN 4:PRINT CHR$(i+ca);:PAPE
R 0:PEN 1:PRINT ": ";
1000 FOR j=2 TO lt
1010 IF g(i,j)=1 THEN PRINT MID$(t$,j-1,
3);",";
1020 NEXT j
1030 PRINT CHR$(8);" "
1040 IF VPOS(#0)<6 THEN GOSUB 8000
1050 NEXT i
1060 GOSUB 8000
1070 GOTO 9999
8000 PRINT:LOCATE 1,25:PRINT "PULSE CUAL
QUIER TECLA."
8010 r$=INKEY$
8020 IF r$="" THEN 8010
8030 IF r$<>"c" THEN 8060
8050 GOTO 8010
8060 IF r$="0" THEN 9999
8070 CLS
8080 RETURN
9999 REM end
```

AYUDA MONOALFABETICA

```
10 REM AYUDA MONOALFABETICA
15 MODE 1
16 CLS
20 LOCATE 9,12:PRINT "PONGA LA CINTA CON
 DATOS":LOCATE 8,13:PRINT "PULSE LUEGO C
UALQUIER TECLA"
30 SOUND 1,239,100
40 CALL &BB18
45 |DISC
46 DIM e(26)
47 DIM t(26,26)
50 'SI FUESE DISCO PONGASE "|DISC" EN 45
51 OPENIN "frec"
52 FOR i=1 TO 26
53 INPUT #9,e(i)
54 NEXT
55 CLOSEIN
56 OPENIN "trans"
57 FOR i=1 TO 26
58 FOR j=1 TO 26
59 INPUT #9,t(i,j)
60 NEXT:NEXT
61 CLOSEIN
70 CLS
80 PRINT "PROGRAMA DE AYUDA MONOALFABETI
CA"
90 LOCATE 3,3:PRINT "TEXTO";
100 INPUT t$
110 IF t$="0" THEN 9999
120 lt=LEN(t$)
130 IF lt>9 THEN 160
140 LOCATE 1,3:PRINT "?"
150 GOTO 90
160 DIM t$(lt):FOR i=1 TO lt:t$(i)=MID$(
t$,i,1):NEXT i
165 FOR i=1 TO lt
170 IF MID$(t$,i,1)<"a" OR MID$(t$,i,1)>
"z" THEN MID$(t$,i,1)=" "
180 NEXT i
190 CLS:PRINT "TEXTO :  ";t$
200 b1=6+INT((lt-1)/15)
210 DIM c(26)
220 ca=ASC("a")-1
230 FOR i=1 TO lt
240 IF MID$(t$,i,1)<>" " THEN c(ASC(MID$
(t$,i,1))-ca)=c(ASC(MID$(t$,i,1))-ca)+1/
lt
250 NEXT i
260 GOSUB 8000
265 CLS
270 FOR i=1 TO 26
275 IF i>=14 THEN LOCATE 20,i-13
280 PAPER 5:PEN 4:PRINT CHR$(i+ca);
285 PAPER 0:PEN 1:PRINT ": ";c(i)*100
290 NEXT i
300 GOSUB 8000
310 DIM a$(26),b$(26),p$(lt)
315 FOR i=1 TO 26:a$(i)="*":b$(i)="*":NE
XT i
320 CLS
330 PLOT 104,392
340 DRAWR 432,0
350 DRAWR 0,-48
360 DRAWR -432,0
370 DRAWR 0,48
380 LOCATE 8,2:PRINT "ABCDEFGHIJKLMNOPQR
STUVWXYZ":LOCATE 8,3:FOR x=1 TO 26:PRINT
 a$(x);:NEXT x:PRINT:PRINT
385 p$=""
390 FOR i=0 TO 15*INT((lt-1)/15) STEP 15
400 j=15
410 IF i+j>lt THEN j=lt-i
420 PRINT MID$(t$,i+1,j);TAB(18);CHR$(12
4);TAB(20);
430 FOR w=1 TO j
440 c$=" "
```

```
450 IF t$(i+w)<>" " THEN c$=a$(ASC(t$(i+
w))-ca)
460 p$(i+w)=c$
470 PRINT c$;
480 NEXT w
485 PRINT
490 NEXT i
500 LOCATE 1,25:PRINT "PULSE b,d,e,f,n,p
,s,t o v"
510 r$=INKEY$
520 IF r$="" THEN 510
530 LOCATE 1,23
540 IF r$<>"b" THEN 920
550 GOSUB 8100
560 GOSUB 8200
570 PAPER 5:PEN 4:PRINT CHR$(l+64);
572 PAPER 0:PEN 1:PRINT ": ";"Frecuencia
: ";c(l)
575 IF c(l)=0 THEN 910
580 b=1
590 FOR i=1 TO 26
600 IF ABS(e(i)-c(l))>b THEN 630
610 b=ABS(e(i)-c(l))
620 p=i
630 NEXT i
635 DIM b$(p)
640 PRINT:PRINT "Sugerencia: ":PAPER 5:P
EN 4:b$(p)="*":PRINT CHR$(p+ca):PAPER 0:
PEN 1:PRINT:PRINT "Transiciones:",
650 DIM n(26)
655 ERASE b$
660 FOR i=2 TO lt
670 IF MID$(t$,i,1)<>l$ THEN 800
680 j=0
683 j=j+1
687 IF i-j<1 THEN 800
690 IF MID$(p$,i-j,1)="*" THEN 800
695 IF MID$(p$,i-j,1)=" " THEN 683
700 t=ASC(MID$(p$,i-j,1))-ca
710 FOR j=1 TO 26
720 n(j)=n(j)+t(t,j)
730 NEXT j
800 NEXT i
810 FOR i=2 TO (19-bl)*2
820 b=0
830 FOR j=1 TO 26
840 IF n(j)<=b THEN 870
850 b=n(j)
860 p=j
870 NEXT j
880 IF b=0 THEN 905
890 PAPER 5:PEN 4:b$(p)="*":PRINT CHR$(p
+ca):PAPER 0:PEN 1:PRINT ": ";n(p),
895 n(p)=0
900 NEXT i
905 ERASE n
910 GOTO 500
920 IF r$<>"c" THEN 950
930 PRINT #8
940 GOTO 500
950 IF r$<>"d" THEN 990
960 GOSUB 8200
965 IF a$(l)<>"*" THEN b$(ASC(a$(l))-ca)
="*"
970 a$(l)="*"
980 GOTO 320
990 IF r$<>"e" THEN 1040
1000 GOSUB 8100
1010 GOSUB 8200
1020 PRINT l$;": ";e(l)
1030 GOTO 500
1040 IF r$<>"f" THEN 1090
1050 GOSUB 8100
1060 GOSUB 8200
1070 PRINT l$;": ";c(l)
1080 GOTO 500
1090 IF r$<>"n" THEN 1100
1095 RUN
1100 IF r$<>"p" THEN 1200
1110 GOSUB 8100
1120 CLS:INPUT "Letras";l$
1130 IF l$="0" THEN 9999
1140 IF LEN(l$)<>2 THEN 1120
1150 l1=ASC(LEFT$(l$,1))-ca
1160 l2=ASC(MID$(l$,2,1))-ca
1170 IF l1<1 OR l1>26 OR l2<1 OR l2>26 T
HEN 1120
1180 PRINT l$;": ";t(l1,l2)
1190 GOTO 500
1200 IF r$<>"s" THEN 1240
1210 FOR i=4 TO 21
1213 LOCATE 1,i+1:PRINT TAB(40);" "
1217 NEXT i
1220 LOCATE 1,5:FOR x=1 TO lt:PRINT p$(x
);:NEXT x:PRINT
1230 GOTO 9999
1240 IF r$<>"t" THEN 1340
1250 GOSUB 8200
1260 q$=l$
1270 l1=1
1280 GOSUB 8200
1300 IF b$(l)<>"*" THEN 1280
1310 IF a$(l1)<>"*" THEN b$(ASC(a$(l1))-
ca)="*"
1320 a$(l1)=l$
1325 b$(l)=q$
1330 GOTO 320
1340 IF r$="0" THEN 9999
1350 LOCATE 1,25:PRINT "?"
1360 SOUND 1,478,100
1370 GOTO 500
8000 LOCATE 9,25:PRINT "PULSE CUALQUIER
TECLA."
8010 r$=INKEY$
8020 IF r$="" THEN 8010
8030 IF r$="0" THEN 9999
8040 IF r$<>"c" THEN RETURN
8060 GOTO 8010
8100 FOR i=bl TO 25
8110 LOCATE 1,i+1:PRINT TAB(40);" "
8120 NEXT i
8130 LOCATE 1,bl+1
8140 RETURN
0200 CLS:INPUT "Letra";l$
8210 IF l$="0" THEN 9999
8220 IF LEN(l$)<>1 THEN 8200
8230 l=ASC(l$)-ca
8240 IF l<1 OR l>26 THEN 8200
8250 RETURN
8300 t$="":FOR x=1 TO lt:t$=t$+t$(x):NEX
T x:RETURN
9999 REM fin
```

ZIG-ZAG

```
10 REM ZIG ZAG
15 MODE 1
16 CLS
20 PRINT "PROGRAMA DE CIFRADO 'ZIG ZAG'"
30 LOCATE 3,3:PRINT "MODO Y CLAVE";
40 INPUT m$
50 IF m$="0" THEN 9999
60 IF LEN(m$)<2 THEN 110
70 IF LEFT$(m$,1)<"c" OR LEFT$(m$,1)>"d"
 THEN 110
75 FOR i=2 TO LEN(m$)
80 IF MID$(m$,i,1)<"0" OR MID$(m$,i,1)>"
9" THEN 110
90 NEXT i
100 GOTO 130
110 LOCATE 1,3:PRINT "?"
120 GOTO 30
130 k=VAL(MID$(m$,2,LEN(m$)))
140 IF k<2 THEN 110
150 LOCATE 1,3:PRINT "MODO : ";LEFT$(m$,
1);" CLAVE : ";k
160 LOCATE 3,5:PRINT "TEXTO";
170 INPUT t$
171 FOR i=2 TO LEN(t$)
172 IF i<LEN (t$) THEN IF MID$(t$,i,1)="
 " THEN t$=LEFT$(t$,i-1)+MID$(t$,i+1,LEN
(t$)):GOTO 172
173 NEXT i
175 IF t$="0" THEN 9999
180 lt=LEN(t$)
190 IF lt>0 THEN 220
200 LOCATE 1,5:PRINT "?";
210 GOTO 170
220 CLS:LOCATE 1,1:PRINT "TEXTO :  ";t$
230 PRINT
235 PRINT "CLAVE: ";k
236 PRINT
240 s=2*(k-1)
250 IF LEFT$(m$,1)="d" THEN 390
260 FOR i=1 TO lt STEP s
270 PRINT MID$(t$,i,1);
275 NEXT i
280 FOR i=1 TO k-2
290 FOR j=1 TO lt STEP s
300 IF j+i<=lt THEN PRINT MID$(t$,j+i,1)
;
310 IF j+s-i<=lt THEN PRINT MID$(t$,j+s-
i,1);
330 NEXT j
340 NEXT i
350 FOR i=k TO lt STEP s
360 PRINT MID$(t$,i,1);
370 NEXT i
380 GOTO 9999
390 DIM c$(lt)
400 l=0
410 FOR i=1 TO lt STEP s
420 l=l+1
430 c$(i)=MID$(t$,l,1)
440 NEXT i
450 FOR i=1 TO k-2
460 FOR j=1 TO lt STEP s
470 IF j+i>lt THEN 500
480 l=l+1
490 c$(i+j)=MID$(t$,l,1)
500 IF J+S-I>LT THEN GOTO 540
510 L=L+1
520 C$(J+S-I)=MID$(T$,L,1)
540 NEXT j
550 NEXT i
560 FOR i=k TO lt STEP s
570 l=l+1
580 c$(i)=MID$(t$,l,1)
590 NEXT i
600 FOR i=1 TO lt:PRINT c$(i);:NEXT i
610 LOCATE 3,22:PRINT "Pulse 's' para se
guir                          'n' para de
tenerse"
620 r$=INKEY$
630 IF r$="" THEN 620
640 IF r$="s" THEN 680
650 IF r$="n" THEN 9999
660 LOCATE 1,23:PRINT "?";
670 GOTO 620
680 ERASE c$:k=k+1
700 GOTO 220
9999 REM fin
```

COLUMNAS COMPLETAS

```
10 REM COLUMNAS COMPLETAS
15 MODE 1
20 PRINT "PROGRAMA DE CIFRADO 'COLUMNAS
COMPLETAS'"
30 LOCATE 3,3:PRINT "MODO Y PALABRA CLAV
E";
40 INPUT m$
50 IF m$="0" THEN 9999
60 IF LEN(m$)<3 THEN 80
70 IF LEFT$(m$,1)="d" OR LEFT$(m$,1)="c"
THEN 100
80 LOCATE 1,3:PRINT "?"
90 GOTO 30
100 k$=MID$(m$,2,LEN(m$))
105 LOCATE 1,3:PRINT "MODO : ";LEFT$(m$,
1);" PALABRA CLAVE : ";k$
107 cc=ASC("(")
110 lk=LEN(k$)
```

```
120 DIM k(lk)
130 FOR i=1 TO lk
140 b=cc
160 FOR j=1 TO lk
170 IF ASC(MID$(k$,j,1))>=b THEN 200
180 b=ASC(MID$(k$,j,1))
190 p=j
200 NEXT j
210 MID$(k$,p,1)="("
215 k(i)=p
220 NEXT i
230 LOCATE 3,5:PRINT "TEXTO";
240 INPUT t$
250 FOR i=2 TO LEN(t$)
260 IF i>=LEN(t$) THEN 300
270 IF MID$(t$,i,1)<>" " THEN 300
280 t$=LEFT$(t$,i-1)+MID$(t$,i+1,LEN(t$))
290 GOTO 260
300 NEXT i
310 IF t$="0" THEN 9999
320 IF LEN(t$)>0 THEN 350
330 LOCATE 1,5:PRINT "?";
340 GOTO 240
350 lt=LEN(t$)
360 IF lt/lk=INT(lt/lk) THEN 390
370 t$=t$+"z"
380 GOTO 350
390 LOCATE 3,5:CLS:PRINT "TEXTO : ";t$
400 PRINT:PRINT
410 IF LEFT$(m$,1)="d" THEN 480
420 FOR i=1 TO lk
430 FOR j=k(i) TO lt STEP lk
440 PRINT MID$(t$,j,1);
450 NEXT j
460 NEXT i
470 GOTO 9999
480 DIM c$(lt)
490 l=0
500 FOR i=1 TO lk
510 FOR j=k(i) TO lt STEP lk
520 l=l+1
530 c$(j)=MID$(t$,l,1)
540 NEXT j
550 NEXT i
560 FOR i=0 TO lt-1:PRINT c$(i);:NEXT
9999 REM fin
```

TRANSPOSICION DE ITINERARIO

```
10 REM TRANSPOSICION DE ITINERARIO
15 MODE 1
16 CLS
20 DIM l$(50)
30 FOR r=1 TO 32
40 READ l$(r)
50 NEXT r
60 DATA afkpubglqvchmrwdinsxejoty
70 DATA upkfavqlgbwrmhcxsnidytoje
80 DATA ejotydinsxchmrwbglqvafkpu
90 DATA ytojexsnidwrmhcvqlgbupkfa
100 DATA abcdefghijklmnopqrstuvwxy
110 DATA uvwxypqrstklmnofghijabcde
120 DATA edcbajihgfonmlktsrqpyxwvu
130 DATA ywxvutsrqponmlkjihgfedcba
140 DATA osvxyjnruwfimqtcehlpabdgk
150 DATA ojfcasniebvrmhdxuqlgywtpk
160 DATA acfjobeinsdhmrvglquxkptwy
170 DATA yxvsowurnjtqmifplheckgdba
180 DATA kptwyglquxdhmrvbeinsacfjo
190 DATA kgdbaplhectqmifwurnjyxvso
200 DATA abdgkcehlpfimqtjnruwosvxy
210 DATA ywtpkxuqlgvrmhdsniebojfca
220 DATA efopydgnqxchmrwbilsvajktu
230 DATA ypofexqngdwrmhcvslibutkja
240 DATA ajktubilsvchmrwdgnqxefopy
250 DATA utkjavslibwrmhcxqngdypofe
260 DATA abcdejihgfklmnotsrqpuvwxy
270 DATA uvwxytsrqpklmnojihgfabcde
280 DATA edcbafghijonmlkpqrstyxwvu
290 DATA yxwvupqrstonmlkfghijedcba
300 DATA abfgocehnpdimqvjlruwkstxy
310 DATA yxtskwurljvqmidpnhecogfba
320 DATA acdjkbeilsfhmrtgnquxopvwy
330 DATA ywvpoxuqngtrmhfsliebkjdca
340 DATA opvwygnquxfhmrtbeilsacdjk
350 DATA kjdcasliebtrmhfxuqngywvpo
360 DATA kstxyjlruwdimqvcehnpabfgo
370 DATA ogfbapnhecvqmidwurljyxtsk
375 DEF FNa=22701+x+32*y
377 ca=ASC("a")-1
380 CLS
390 PRINT "TRANSPOSICION DE ITINERARIO"
400 LOCATE 3,3:PRINT "MODO (NUMERO CLAVE
)";
410 INPUT m$
420 IF m$="0" THEN 9999
430 IF m$="1" THEN 1010
440 IF m$="s" THEN 1510
450 lm=LEN(m$)
460 IF lm<2 THEN 520
470 IF LEFT$(m$,1)<"c" OR LEFT$(m$,1)>"d
" THEN 520
480 FOR i=2 TO lm
490 IF MID$(m$,i,1)<"0" OR MID$(m$,i,1)>
"9" THEN 520
500 NEXT i
510 GOTO 540
520 LOCATE 1,3:PRINT "?"
530 GOTO 400
540 k=VAL(MID$(m$,2,LEN(m$)))
550 IF k<1 OR k>=r THEN 520
560 LOCATE 1,3:PRINT "MODO : ";LEFT$(m$,
1);" NUMERO CLAVE : ";k
```

```
561 LOCATE 1,5:PRINT "ITINERARIO :"
562 FOR y=0 TO 4
563 LOCATE 15,5+y:PRINT MID$(l$(k),y*5+1
,5)
564 NEXT y
565 PLOT 216,344
566 DRAWR 96,0
567 DRAWR 0,-96
568 DRAWR -96,0
569 DRAWR 0,96
570 LOCATE 3,11:PRINT "TEXTO";
580 INPUT t$
590 FOR i=1 TO LEN(t$)
600 IF i>LEN(t$) THEN 670
610 IF MID$(t$,i,1)<>" " THEN 670
620 r$=""
630 IF i>1 THEN r$=LEFT$(t$,i-1)
640 IF i<LEN(t$) THEN r$=r$+MID$(t$,i+1,
LEN(t$))
650 t$=r$
660 GOTO 600
670 NEXT i
680 IF t$="0" THEN 9999
690 lt=LEN(t$)
700 IF lt>0 THEN 730
710 LOCATE 1,11:PRINT "?"
720 GOTO 580
730 IF lt/25=INT(lt/25) THEN 770
740 t$=t$+"z"
750 lt=lt+1
760 GOTO 730
770 CLS:PRINT "TEXTO : ";t$
780 PRINT:PRINT
790 IF LEFT$(m$,1)="d" THEN 910
800 c$="                                "
810 FOR i=1 TO 25
820 FOR j=1 TO 25
830 IF MID$(l$(k),j,1)<>CHR$(ca+i) THEN
840
835 c$=LEFT$(c$,j-1)+MID$(t$,i,1)+MID$(c
$,j+1)
840 NEXT j
850 NEXT i
860 PRINT c$;
870 IF lt<=25 THEN 9999
880 t$=MID$(t$,26,LEN(t$))
890 lt=lt-25
900 GOTO 800
910 DIM c$(26)
920 FOR i=1 TO 25
930 FOR j=1 TO 25
940 IF MID$(l$(k),j,1)<>CHR$(ca+i) THEN
950
945 c$=LEFT$(c$,i-1)+MID$(t$,j,1)+MID$(c
$,i+1)
950 NEXT j
960 NEXT i
970 PRINT c$;
975 IF lt=25 THEN 9999
980 t$=MID$(t$,26,LEN(t$))
990 lt=lt-25
995 ERASE c$
1000 GOTO 910
1010 IF r<=50 THEN 1070
1020 LOCATE 1,3:PRINT "?"
1030 LOCATE 1,5:PRINT "LIBRERIA COMPLETA
"
1040 SOUND 1,478,100
1050 LOCATE 1,5:PRINT TAB(22)
1060 GOTO 410
1065 ERASE c$
1070 LOCATE 1,3:PRINT "NUMERO DE ITINERA
RIO :  ";r;" "
1080 FOR x=0 TO 4
1090 LOCATE 10,10+x
1095 INPUT m$(x)
1100 IF LEN (m$(x))<>5 THEN SOUND 1,478,
100:GOTO 1090
1110 FOR y=1 TO 5
1120 IF  MID$(m$(x),y,1)<"a" OR MID$(m$(
x),y,1)>"z" THEN SOUND 1,478,100:GOTO 10
90
1130 NEXT y
1140 NEXT x
1150 c$=""
1160 FOR x=0 TO 4
1170 c$=c$+m$(X)
1180 NEXT X
1190 FOR X=2 TO 25
1200 FOR Y=1 TO X-1
1210 IF MID$(C$,X,1)=MID$(C$,Y,1) THEN G
OTO 1080
1220 NEXT Y
1230 NEXT X
1240 L$(R)=C$
1495 R=R+1
1500 GOTO 380
1510 LOCATE 3,3:PRINT "NOMBRE";TAB(26);
1520 INPUT r$
1525 LOCATE 1,3:PRINT "NOMBRE : ";r$
1540 GOTO 380
9999 REM end
```

REJILLA DE CARDANO

```
10 REM REJILLA DE CARDANO
15 MODE 1
16 CLS
20 PRINT "PROGRAMA DE CIFRADO 'REJILLA D
E CARDANO'"
30 LOCATE 3,3:PRINT "MODO";
40 INPUT m$
50 IF m$="0" THEN 9999
60 IF m$="d" OR m$="c" THEN 90
70 LOCATE 1,3:PRINT "?"
80 GOTO 30
90 LOCATE 2,3:PRINT "MODO : ";m$
97 nh=0
110 PLOT 504,232:DRAWR -128,0
```

```
120 PLOT 504,232:DRAWR 0,128:DRAWR -128,
0:DRAWR 0,-128
130 PLOT 440,296
140 DRAWR 64,0
150 PLOT 440,296:DRAWR 0,-64
160 PLOT 440,296:DRAWR -64,0
170 PLOT 440,296:DRAWR 0,64
190 FOR q=1 TO 4
200 sx=24
210 IF q=2 OR q=3 THEN sx=28
220 sy=3
230 IF q>2 THEN sy=7
240 LOCATE sx+1,sy+1:PRINT "123":LOCATE
sx+1,sy+2:PRINT "456":LOCATE sx+1,sy+3:P
RINT "789"
250 LOCATE 1,5:PRINT "CUADRANTE";q;"AGUJ
ERO  "
260 LOCATE 23,5:PRINT " ";CHR$(8);
270 r$=INKEY$
280 IF r$="" THEN 270
290 IF r$="0" THEN 9999
300 IF r$="n" THEN 620
310 IF r$>="1" AND r$<="9" THEN 350
320 LOCATE 15,5:PRINT "?"
330 SOUND 1,478,100
340 GOTO 260
350 v=VAL(r$)
360 LOCATE 20,5:PRINT v
370 gy=INT((v-1)/3)+1
380 gx=v-3*(gy-1)
390 IF q=2 OR q=3 THEN gx=gx+3
400 IF q>2 THEN gy=gy+3
410 IF g(gy,gx)=1 THEN 330
420 FOR y=1 TO 6
430 FOR x=1 TO 6
440 IF g(y,x)=0 THEN 530
450 yy=y
460 xx=x
470 FOR r=1 TO q-1
480 i=yy
490 yy=xx
500 xx=7-i
510 IF yy=gy AND xx=gx THEN 330
520 NEXT r
530 NEXT x
540 NEXT y
550 g(gy,gx)=1
560 IF gx>3 THEN gx=gx+1
570 IF gy>3 THEN gy=gy+1
580 LOCATE 24+gx,3+gy:PRINT CHR$(143)
590 nh=nh+1
600 IF nh<9 THEN 260
610 q=4
620 IF q=4 AND nh<9 THEN 320
680 NEXT q
690 LOCATE 1,5:PRINT TAB(22)
700 LOCATE 3,13:PRINT "TEXTO";
710 INPUT t$
720 FOR i=1 TO LEN(t$)
730 IF i>LEN(t$) THEN 800
740 IF MID$(t$,i,1)<>" " THEN 800
750 r$=""
760 IF i>1 THEN r$=LEFT$(t$,i-1)
770 IF i<LEN(t$) THEN r$=r$+MID$(t$,i+1,
LEN(t$))
780 t$=r$
790 GOTO 730
800 NEXT i
810 IF t$="0" THEN 9999
820 lt=LEN(t$)
830 IF lt/36=INT(lt/36) THEN 870
840 t$=t$+"z"
850 lt=lt+1
860 GOTO 830
870 LOCATE 1,13:PRINT "TEXTO : ";t$
880 PRINT
890 DIM c$(6,6)
895 rf=1
900 IF m$="d" THEN 1110
910 cn=0
920 FOR q=1 TO 4
930 FOR y=1 TO 6
940 FOR x=1 TO 6
950 IF g(y,x)=0 THEN 980
960 cn=cn+1
970 c$(y,x)=MID$(t$,cn,1)
980 NEXT x
990 NEXT y
1000 GOSUB 2000
1010 NEXT q
1020 FOR y=1 TO 6
1030 FOR x=1 TO 6
1040 PRINT c$(y,x);
1050 NEXT x
1060 NEXT y
1070 IF lt=36 THEN 9999
1080 t$=MID$(t$,37,LEN(t$))
1090 lt=lt-36
1100 GOTO 910
1110 cn=0
1120 FOR y=1 TO 6
1130 FOR x=1 TO 6
1140 cn=cn+1
1150 c$(y,x)=MID$(t$,cn,1)
1160 NEXT x
1170 NEXT y
1180 FOR q=1 TO 4
1190 FOR y=1 TO 6
1200 FOR x=1 TO 6
1210 IF g(y,x)>0 THEN PRINT c$(y,x);
1220 NEXT x
1230 NEXT y
1240 GOSUB 2000
1250 NEXT q
1260 IF lt=36 THEN 9999
1270 t$=MID$(t$,37,LEN(t$))
1280 lt=lt-36
1290 GOTO 1110
2000 FOR y=1 TO 6
2010 FOR x=1 TO 6
2020 IF g(y,x)<>rf THEN 2070
2030 g(y,x)=0
2040 yy=x
2050 xx=7-y
2060 g(yy,xx)=3-rf
2070 NEXT x
2080 NEXT y
2090 rf=3-rf
2100 RETURN
9999 REM end
```

ANALISIS POR COLUMNAS COMPLETAS

```
10 REM ANALISIS POR COLUMNAS COMPLETAS
15 nr=30:nc=15:DIM c$(nr,nc),p$(nr,nc),b
(nc),f(nc),e(26),t(26,26)
16 MODE 1:CLS
20 LOCATE 9,12:PRINT "PONGA LA CINTA CON
 DATOS":LOCATE 8,13:PRINT "PULSE LUEGO C
UALQUIER TECLA"
30 SOUND 1,239,100
40 CALL &BB18
50 |TAPE
51 'SI EL FICHERO SE ENCUENTRA EN DISCO
SE PONDRA "|DISC" EN 50
52 OPENIN "frec"
53 FOR i=1 TO 26
54 INPUT #9,e(i)
55 NEXT
56 CLOSEIN
57 OPENIN "trans"
58 FOR i=1 TO 26
59 FOR j=1 TO 26
60 INPUT #9,t(i,j)
61 NEXT:NEXT
62 CLOSEIN
70 CLS
80 PRINT "ANALISIS POR COLUMNAS COMPLETA
S"
90 LOCATE 3,3:PRINT "TEXTO";
100 INPUT t$
110 FOR i=1 TO LEN(t$)
120 IF i>LEN(t$) THEN 190
125 IF MID$(t$,i,1)="A" AND MID$(t$,i,1)
="Z" THEN MID$(t$,i,1)=CHR$(ASC(MID$(t$,
i,1))+ASC("a")-ASC("A"))
130 IF MID$(t$,i,1)<>" " THEN 190
140 r$=""
150 IF i>1 THEN r$=LEFT$(t$,i-1)
160 IF i<LEN(t$) THEN r$=r$+RIGHT$(t$,LE
N(t$)-i)
170 t$=r$
180 GOTO 120
190 NEXT i
200 IF t$="0" THEN 9999
210 lt=LEN(t$)
220 IF lt>0 THEN 250
230 LOCATE 1,3:PRINT "?"
240 GOTO 90
250 nf=0
260 FOR i=2 TO INT(lt/2)
270 IF lt/i=INT(lt/i) THEN nf=nf+1
280 NEXT i
290 IF nf=0 THEN 230
300 DIM c(nf)
310 DIM r(nf)
320 nf=0
330 FOR i=2 TO INT(lt/2)
340 IF lt/i >INT(lt/i) THEN 380
350 nf=nf+1
360 c(nf)=i
370 r(nf)=lt/i
380 NEXT i
385 ca=ASC("a")-1
390 CLS:PRINT "TEXTO: ";t$
400 PRINT
410 PRINT "HAY";nf;"MODOS POSIBLES DE FA
CTORIZACION"
420 PRINT
430 FOR i=1 TO nf
440 PAPER 5:PEN 4:PRINT i:PAPER 0:PEN 1:
PRINT ": ";c(i);" columnas, ";r(i);" fil
as."
445 NEXT i
450 PRINT
460 PRINT "DISTRIBUCION DE VOCALES (S/N/
O)"
475 SOUND 1,319,50
480 r$=INKEY$
490 IF r$="" THEN 480
500 IF r$="O" THEN 9999
510 IF r$="n" THEN 650
515 CLS
520 FOR i=1 TO nf
530 PAPER 5:PEN 4:PRINT i:PAPER 0:PEN 1:
PRINT ": ";c(i);"x";r(i);" : ";
540 FOR j=1 TO r(i)
550 nv=0
560 FOR k=1 TO c(i)
570 r$=MID$(t$,(k-1)*r(i)+j,1)
580 IF r$="a" OR r$="e" OR r$="i" OR r$=
"o" OR r$="u" THEN nv=nv+1
590 NEXT k
600 PRINT INT(nv/c(i)*100);"%";
610 NEXT j
620 PRINT
630 PRINT
640 NEXT i
650 PRINT
660 INPUT "NUMERO DE LA OPCION QUE ESCOG
E ";r$
665 bd=VAL(r$)
667 IF bd=0 THEN 9999
670 IF bd<1 OR bd>nf OR bd>INT(bd) THEN
660
680 nc=c(bd)
690 nr=r(bd)
692 FOR i=1 TO nr
693 FOR j=1 TO nc
694 c$(i,j)=MID$(t$,(j-1)*nr+i,1)
695 NEXT j
696 NEXT i
697 FOR i=1 TO nc:f(i)=0:b(i)=0:NEXT i
700 CLS
710 FOR i=1 TO nc
720 LOCATE i,1:PRINT MID$(STR$(INT(i/10)
),2,1):LOCATE 16+i,1:PRINT MID$(STR$(INT
(i/10)),2,1)
730 LOCATE i,2:PRINT MID$(STR$(i-10*INT(
```

```
i/10)),2,1);:LOCATE 16+i,2:PRINT MID$(ST
R$(i-10*INT(i/10)),2,1)
740 LOCATE i,3:PRINT "-":LOCATE 16+i,3:P
RINT "-"
750 NEXT i
760 FOR i=1 TO nr
765 FOR j=1 TO nc
770 PRINT c$(i,j);
775 NEXT j:PRINT
780 NEXT i
790 GOSUB 8000
810 f(cn)=1
820 b(1)=cn
830 GOSUB 8100
840 LOCATE 1,25:PRINT TAB(40):LOCATE 1,2
5:PRINT "PULSE w,d,i,l,r,p,b,s, o 0."
845 LOCATE 1,21:PRINT TAB(40)
850 r$=INKEY$
860 IF r$="" THEN 850
867 IF r$="b" THEN CLS:GOTO 390
890 IF r$="0" THEN 9999
900 IF r$<>"l" AND r$<>"r" THEN 1160
910 GOSUB 8050
915 IF b(pc)=0 THEN 910
920 c=b(pc)
930 GOSUB 8220
1010 FOR i=1 TO nc
1020 IF i=c THEN 1140
1030 PRINT i;
1050 PRINT ":";
1060 p=0
1070 FOR j=1 TO nr
1080 cp=ASC(c$(j,c))-ca
1090 tc=ASC(c$(j,i))-ca
1100 IF r$="l" THEN p=p+t(tc,cp)
1110 IF r$="r" THEN p=p+t(cp,tc)
1120 NEXT j
1130 PRINT p;CHR$(fc);
1140 NEXT i
1150 INPUT "Pulse ENTER:";r$
1151 FOR h=1 TO 8:LOCATE 1,17+h:PRINT TA
B(40):NEXT h
1152 GOSUB 8220
1153 GOTO 840
1160 IF r$<>"d" THEN 1250
1170 GOSUB 8050
1175 IF b(pc)>0 THEN f(b(pc))=0:b(pc)=0
1180 FOR i=pc TO nc-1
1190 b(i)=b(i+1)
1200 IF b(i)>0 THEN f(b(i))=i
1210 NEXT i
1220 b(nc)=0
1230 GOSUB 8100
1240 GOTO 840
1250 IF r$<>"i" THEN 1301
1255 GOSUB 8050
1257 f(b(nc))=0
1259 IF pc>=nc THEN 1290
1260 FOR i=nc TO pc+1 STEP -1
1270 b(i)=b(i-1)
1280 IF b(i)>0 THEN f(b(i))=i
1290 NEXT i
1292 b(pc)=0
1294 GOSUB 8100
1300 GOTO 840
1301 IF r$<>"w" THEN 1310
1302 GOSUB 8050
1303 GOSUB 8000
1304 IF b(pc)>0 THEN f(b(pc))=0
1305 f(cn)=pc
1306 b(pc)=cn
1307 GOSUB 8100
1308 GOTO 840
1310 IF r$<>"p" THEN 1319
1311 LOCATE 2,20:INPUT "Letras:";r$
1312 IF LEN(r$)<>2 THEN 1311
1313 l1=ASC(LEFT$(r$,1))-ca
1314 l2=ASC(RIGHT$(r$,1))-ca
1315 IF l1<1 OR l1>26 OR l2<1 OR l2>26 T
HEN 1311
1316 LOCATE 14,21:PRINT "FREC=";t(l1,l2)
1318 GOTO 840
1319 IF r$="s" THEN 1350
1320 LOCATE 1,25:PRINT "?"
1330 SOUND 1,478,100
1340 GOTO 840
1350 CLS:PRINT "SOLUCION:":PRINT
1360 FOR j=1 TO nr
1365 FOR i=1 TO nc
1370 PRINT c$(j,b(i));
1380 NEXT i:NEXT j
1390 GOTO 9999
8000 LOCATE 1,21:INPUT "Que columna quie
re poner";cn
8010 cn=INT(cn)
8020 IF cn=0 THEN 9999
8030 IF cn<1 OR cn>nc THEN 8000
8035 IF f(cn)>0 THEN 8000
8040 RETURN
8050 LOCATE 1,21:PRINT TAB(40):LOCATE 1,
21:INPUT "En que posicion";pc
8055 LOCATE 1,21:PRINT SPC(40)
8060 pc=INT(pc)
8070 IF pc=0 THEN 9999
8080 IF pc<1 OR pc>nc THEN 8050
8090 RETURN
8100 FOR i=1 TO nr:FOR j=1 TO nc:p$(i,j)
=" ":NEXT j:NEXT i
8110 FOR i=1 TO nc
8115 LOCATE i,3:PRINT "-"
8120 c=f(i)
8130 IF c=0 THEN 8170
8135 LOCATE i,3:PRINT CHR$(203)
8140 FOR j=1 TO nr
8150 p$(j,c)=c$(j,i)
8160 NEXT j
8170 NEXT i
8180 FOR i=1 TO nr
8190 LOCATE 17,3+i:FOR j=1 TO nc:PRINT p
$(i,j);:NEXT j:PRINT
8200 NEXT i
8210 RETURN
8220 sy=nr+4
8230 FOR i=sy TO 20
8240 LOCATE 1,i+1:PRINT TAB(40);" "
8250 NEXT i
8260 RETURN
9999 REM fin
```

ANALISIS POR LA REJILLA DE CARDANO

```
10 REM ANALISIS POR LA REJILLA
              DE CARDANO
15 DIM e(26),t(26,26),g(6,6),a(6,6)
16 MODE 1:CLS
20 LOCATE 9,12:PRINT "PONGA LA CINTA CON
 DATOS":LOCATE 8,13:PRINT "PULSE LUEGO C
UALQUIER TECLA"
30 SOUND 1,239,100
40 CALL &BB18
47 'PARA CARGAR MEDIANTE DISCO PONER |DI
SC EN 50
50 |DISC
51 OPENIN "frec"
52 FOR i=1 TO 26
53 INPUT #9,e(i)
54 NEXT
55 CLOSEIN
56 OPENIN "trans"
57 FOR i=1 TO 26
58 FOR j=1 TO 26
59 INPUT #9,t(i,j)
60 NEXT:NEXT
61 CLOSEIN
70 CLS
80 PRINT "PROGRAMA DE ANALISIS'REJILLA D
E CARDANO'"
90 LOCATE 3,3:PRINT "TEXTO";
100 INPUT t$
110 IF t$="0" THEN 9999
120 FOR i=1 TO LEN(t$)
130 IF i>LEN(t$) THEN 200
140 IF MID$(t$,i,1)>="a" AND MID$(t$,i,1
)<="z" THEN 200
150 r$=""
160 IF i>1 THEN r$=LEFT$(t$,i-1)
170 IF i<LEN(t$) THEN r$=r$+RIGHT$(t$,LE
N(t$)-i)
180 t$=r$
190 GOTO 130
200 NEXT i
210 lt=LEN(t$)
220 IF lt=0 THEN 240
230 IF lt/36=INT(lt/36) THEN 260
235 t$=t$+"z"
240 lt=lt+1
250 GOTO 230
260 FOR h=1 TO 15:LOCATE 1,h+2:PRINT TAB
(40):NEXT h
265 LOCATE 3,3:PRINT "TEXTO: "; t$
270 nb=INT(lt/36)
310 ca=ASC("a")-1
370 LOCATE 1,25:PRINT "PULSE CUALQUIER T
ECLA."
380 r$=INKEY$
390 IF r$="" THEN 380
395 IF r$="0" THEN 9999
400 IF r$<>"c" THEN 430
420 GOTO 380
430 CLS
460 PLOT 248,376
470 DRAWR 112,0
480 DRAWR 0,-112
490 DRAWR -112,0
500 DRAWR 0,112
510 LOCATE 17,1:PRINT "123456";
520 FOR i=1 TO 6
530 LOCATE 13,i+2:PRINT i
540 NEXT i
541 nh=0
545 r$=""
550 GOTO 700
560 LOCATE 1,25:PRINT "PULSE d,h,l,r,p,t
,n o 0"
570 r$=INKEY$
580 IF r$="" THEN 570
590 LOCATE 1,25:PRINT TAB(40)
600 IF r$<>"c" THEN 630
620 GOTO 560
630 IF r$<>"d" THEN 690
640 GOSUB 8000
650 g(y,x)=0
660 LOCATE 16+x,2+y:PRINT " ";
670 nh=nh-1
680 GOTO 560
690 IF r$<>"h" THEN 740
700 GOSUB 8000
710 g(y,x)=1
720 LOCATE 16+x,2+y:PRINT CHR$(143);
725 nh=nh+1
730 GOTO 560
740 IF r$<>"l" AND r$<>"r" THEN 1105
745 GOSUB 8200
750 GOSUB 8000
753 xx=x
757 yy=y
760 IF r$="l" THEN 830
770 x=x+1
780 IF x<=6 THEN 915
790 x=1
800 y=y+1
810 IF y>6 THEN 560
820 GOTO 915
830 x=x-1
840 IF x>=1 THEN 915
850 x=6
860 y=y-1
870 IF y<1 THEN 560
915 p=0
917 FOR i=1 TO nb
920 FOR j=1 TO 2
960 IF r$="r" THEN p=p+t(ASC(MID$(t$,(i-
1)*36+(yy-1)*6+xx,1))-ca,ASC(MID$(t$,(i-
1)*36+(y-1)*6+x,1))-ca)
970 x=7-x
980 y=7-y
990 xx=7-xx
```

```
1000 yy=7-yy
1010 r$=CHR$(ASC("r")+ASC("l")-ASC(r$))
1020 NEXT j
1025 NEXT i
1030 in=1
1040 FOR i=1 TO 4
1050 GOSUB 8100
1060 IF g(x,y)=1 THEN in=0
1070 NEXT i
1080 PRINT x;",";y;":";p,
1090 IF VPOS(#0)>5 OR POS(#0)=17 THEN 76
0
1100 GOTO 560
1105 IF r$="n" THEN 430
1110 IF r$<>"p" THEN 1200
1120 GOSUB 8200
1130 INPUT "Letras";l$
1135 PRINT
1140 IF LEN(l$)<>2 THEN 1130
1150 l1=ASC(LEFT$(l$,1))-ca
1160 l2=ASC(MID$(l$,2,1))-ca
1170 IF l1<1 OR l1>26 OR l2<1 OR l2>26 T
HEN 1130
1180 PAPER 5:PEN 4:PRINT l$:PAPER 0:PEN
1:PRINT ": ";t(l1,l2)
1190 GOTO 560
1200 IF r$<>"t" THEN 1460
1205 IF nh=9 THEN 1210
1207 SOUND 1,478,100
1208 GOTO 560
1210 rf=1
1211 FOR y=1 TO 6
1212 FOR x=1 TO 6
1213 a(y,x)=g(y,x)
1214 NEXT x
1215 NEXT y
1219 FOR i=1 TO 4
1220 GOSUB 8200
1225 FOR j=1 TO nb
1230 FOR k=1 TO 4
1240 FOR y=1 TO 6
1250 FOR x=1 TO 6
1260 IF a(y,x)<>rf THEN 1270
1261 PRINT MID$(t$,(j-1)*36+(y-1)*6+x,1);
1262 a(y,x)=0
1263 a(x,7-y)=3-rf
1270 NEXT x
1280 NEXT y
1290 rf=3-rf
1300 NEXT k
1310 NEXT j
1320 LOCATE 1,25:PRINT "PULSE n,r,s o 0."
1330 r$=INKEY$
1340 IF r$="" THEN 1330
1345 LOCATE 1,25:PRINT TAB(40)
1350 IF r$<>"c" THEN 1380
1370 GOTO 1320
1380 IF r$<>"n" THEN 1410
1381 FOR y=1 TO 6
1382 FOR x=1 TO 6
1383 IF a(y,x)<>rf THEN 1386
1384 a(y,x)=0
1385 a(x,7-y)=3-rf
1386 NEXT x
1387 NEXT y
1388 rf=3-rf
1390 NEXT i
1400 GOTO 1219
1410 ERASE g,a:IF r$="r" THEN 560
1420 IF r$="s" OR r$="0" THEN 9999
1430 LOCATE 1,25:PRINT "?"
1440 SOUND 1,478,100
1450 GOTO 1320
1460 IF r$="0" THEN 9999
1470 LOCATE 1,25:PRINT "?"
1480 SOUND 1,478,100
1490 GOTO 560
8000 LOCATE 1,15:INPUT "Posicion:x,y";x,
y
8005 IF x=0 OR y=0 THEN 9999
8010 IF x<1 OR x>6 OR x>INT(x) OR y<1 OR
 y>6 OR y>INT(y) THEN 8000
8020 IF r$="d" OR r$="l" OR r$="r" THEN
8080
8030 FOR i=1 TO 4
8040 GOSUB 8100
8050 IF g(y,x)<>0 THEN 8090
8060 NEXT i
8070 RETURN
8080 IF g(y,x)=1 THEN 8070
8090 SOUND 1,478,100
8095 GOTO 8000
8100 s=y
8110 y=7-x
8120 x=s
8130 RETURN
8200 FOR i=10 TO 20
8210 LOCATE 1,i+1:PRINT TAB(40);" "
8220 NEXT i
8230 LOCATE 1,11
8240 RETURN
9999 REM fin
```

HILL

```
10 REM HILL
15 MODE 1
16 CLS
17 DATA 1,9,21,15,3,19,0,7,23,11,5,17,25
20 PRINT "PROGRAMA DE CIFRADO 'HILL'"
30 LOCATE 3,3:PRINT "MODO";
40 INPUT m$
50 IF m$="0" THEN 9999
60 IF m$="c" OR m$="d" THEN 90
70 LOCATE 1,3:PRINT "?"
80 GOTO 30
90 LOCATE 1,3:PRINT " MODO : ";m$
100 LOCATE 3,5:PRINT "MATRIZ";
110 INPUT a,b,c,d
```

```
115 CLS
120 LOCATE 1,6:PRINT TAB (40)
130 l=a*d-b*c
133 GOSUB 1000
137 det=l
140 IF l<>0 THEN 180
150 LOCATE 1,3:PRINT "NO EXISTE MATRIZ I
NVERSA"
160 LOCATE 1,5:PRINT "?";
170 GOTO 100
180 IF l/2>INT(l/2) AND l/13>INT(l/13) T
HEN 210
190 LOCATE 1,3:PRINT "EL DETERMINANTE NO
 ES ADECUADO"
200 GOTO 160
210 LOCATE 1,5:PRINT "MATRIZ : ";a;",";b
;",";c;",";d
220 LOCATE 3,7:PRINT "TEXTO";
230 INPUT t$
240 IF t$="0" THEN 9999
260 FOR i=1 TO LEN(t$)
270 IF i>LEN(t$) THEN 330
280 IF MID$(t$,i,1)>="a" AND MID$(t$,i,1
)<="z"THEN 330
290 r$=""
300 IF i>1 THEN r$=LEFT$(t$,i-1)
310 IF i<LEN(t$) THEN r$=r$+MID$(t$,i+1,
LEN(t$))
320 t$=r$
325 GOTO 270
330 NEXT i
340 lt=LEN(t$)
350 IF lt>1 THEN 380
360 LOCATE 1,7:PRINT "?";
370 GOTO 220
380 IF lt/2=INT(lt/2) THEN 410
390 t$=t$+"z"
400 lt=lt+1
410 LOCATE 1,7:CLS:PRINT "TEXTO : ";t$
415 ca=ASC("a")-1
420 IF m$="c" THEN 500
425 FOR i=1 TO 25 STEP 2
426 READ j
427 IF i=det THEN r=j
428 NEXT i
430 i=a
433 a=d
437 d=i
440 b=-b
445 c=-c
450 l=a*r
453 GOSUB 1000
457 a=l
460 l=b*r
463 GOSUB 1000
464 b=l
465 l=c*r
466 GOSUB 1000
467 c=l
470 l=d*r
473 GOSUB 1000
477 d=l
480 PRINT
490 PRINT "MATRIZ INVERSA : ";a",";b;","
;c;",";d
500 PRINT
510 FOR i=1 TO lt STEP 2
520 l1=ASC(MID$(t$,i,1))-ca
530 l2=ASC(MID$(t$,i+1,1))-ca
540 l=a*l1+b*l2
550 GOSUB 1000
560 PRINT CHR$(l1+ca);
570 l=c*l1+d*l2
580 GOSUB 1000
590 PRINT CHR$(l1+ca);
600 NEXT i
610 GOTO 9999
1000 IF l>=0 AND l<26 THEN 1040
1010 IF l<0 THEN l=l+26
1020 IF l>=26 THEN l=l-26
1030 GOTO 1000
1040 l1=l
1050 IF l=0 THEN l1=26
1060 RETURN
9999 REM end
```

GRONSFELD

```
10 REM GRONSFELD
15 MODE 1
16 CLS
20 PRINT "PROGRAMA DE CIFRADO 'GRONSFELD
'"
30 LOCATE 3,3:PRINT "MODO Y NUMERO CLAVE
";
40 INPUT m$
50 IF m$="0" THEN 9999
60 lm=LEN(m$)
70 IF lm<2 THEN 90
80 IF LEFT$(m$,1)="c" OR LEFT$(m$,1)="d"
THEN 110
90 LOCATE 1,3:PRINT "?"
100 GOTO 30
110 DIM k(lm-1)
120 FOR i=2 TO lm
130 k$=MID$(m$,i,1)
140 IF k$<"0" OR k$>"9" THEN 90
150 k(i-1)=VAL(k$)
160 NEXT i
170 LOCATE 1,3:PRINT "MODO : ";LEFT$(m$,
1);" NUMERO CLAVE : ";MID$(m$,2,LEN(m$))
180 LOCATE 3,5:PRINT "TEXTO";
190 INPUT t$
200 IF t$="0" THEN 9999
210 lt=LEN(t$)
220 IF lt>0 THEN 250
230 LOCATE 1,5:PRINT "?"
240 GOTO 190
```

```
250 CLS:LOCATE 1,1:PRINT "TEXTO : ";t$
260 PRINT
263 cs=ASC(" ")
265 ca=ASC("a")
267 cz=ASC("z")
270 IF LEFT$(m$,1)="d" THEN 370
280 k=0
290 FOR i=1 TO lt
293 IF MID$(t$,i,1)<>" " THEN 300
295 l=cs
297 GOTO 340
300 k=k+1
310 IF k=lm THEN k=1
320 l=ASC(MID$(t$,i,1))+k(k)
330 IF l>cz THEN l=l-26
340 PRINT CHR$(l);
350 NEXT i
360 GOTO 9999
370 k=0
380 FOR i=1 TO lt
383 IF MID$(t$,i,1)<>" " THEN 390
385 l=cs
387 GOTO 430
390 k=k+1
400 IF k=lm THEN k=1
410 l=ASC(MID$(t$,i,1))-k(k)
420 IF l<ca THEN l=l+26
430 PRINT CHR$(l);
440 NEXT i
9999 REM end
```

BIFIDO

```
10 REM BIFIDO
15 MODE 1
16 CLS
20 PRINT "PROGRAMA DE CIFRADO 'BIFIDO'"
30 LOCATE 3,3:PRINT "MODO Y PALABRA CLAV
E";
40 INPUT m$
50 IF m$="0" THEN 9999
60 IF LEN(m$)<2 THEN 80
70 IF LEFT$(m$,1)="c" OR LEFT$(m$,1)="d"
THEN 100
80 LOCATE 1,3:PRINT "?"
90 GOTO 30
100 DIM a(25)
110 DIM l(25)
115 ca=ASC("a")-1
120 a=0
130 FOR i=2 TO LEN(m$)
140 c=ASC(MID$(m$,i,1))-ca
150 IF l(c)>0 THEN 190
160 a=a+1
170 a(a)=c
180 l(c)=a
190 NEXT i
200 FOR i=1 TO 25
210 IF l(i)>0 THEN 250
220 a=a+1
230 a(a)=i
240 l(i)=a
250 NEXT i
260 LOCATE 1,3:PRINT "MODO : ";LEFT$(m$,
1);TAB (40)
270 LOCATE 1,5:PRINT "ALFABETO ALTERADO:"
280 FOR i=0 TO 4
290 FOR j=1 TO 5
300 LOCATE 21+j,5+i:PRINT CHR$(a(i*5+j)+
ca)
310 NEXT j
320 NEXT i
330 LOCATE 3,11:PRINT "LONGITUD DEL BLOQ
UE";
340 INPUT b
345 IF b=0 THEN 9999
350 IF b>1 AND b=INT(b) THEN 380
360 LOCATE 1,11:PRINT "?"
370 GOTO 330
380 LOCATE 1,11:PRINT "LONGITUD DEL BLOQ
UE : ";b
385 DIM b(2*b)
390 LOCATE 3,13:PRINT "TEXTO";
400 INPUT t$
405 IF t$="0" THEN 9999
410 FOR i=1 TO LEN(t$)
420 IF i>LEN(t$) THEN 490
430 IF MID$(t$,i,1)>="a" AND MID$(t$,i,1
)<="y" THEN 490
440 r$=""
450 IF i>1 THEN r$=LEFT$(t$,i-1)
460 IF i<LEN(t$) THEN r$=r$+MID$(t$,i+1,
LEN(t$))
470 t$=r$
480 GOTO 420
490 NEXT i
500 lt=LEN(t$)
510 IF lt>1 THEN 540
520 LOCATE 1,13:PRINT "?"
530 GOTO 390
540 CLS: LOCATE 1,1:PRINT "TEXTO : ";t$
550 PRINT
560 IF LEFT$(m$,1)="d" THEN 720
570 FOR i=1 TO lt STEP b
580 t=b-1
590 IF i+t>lt THEN t=lt-i
600 FOR j=0 TO t
610 l=ASC(MID$(t$,i+j,1))-ca
620 a=l(l)
630 b(j+1)=INT((a-1)/5)+1
640 b(j+t+2)=a-5*(b(j+1)-1)
650 NEXT j
660 FOR j=0 TO 2*t STEP 2
670 c=(b(j+1)-1)*5+b(j+2)
680 PRINT CHR$(a(c)+ca);
690 NEXT j
700 NEXT i
710 GOTO 9999
720 FOR i=1 TO lt STEP b
```

```
730 t=b-1
740 IF i+t>lt THEN t=lt-i
750 FOR j=0 TO t
760 c=ASC(MID$(t$,i+j,1))-ca
770 a=l(c)
780 b(j*2+1)=INT((a-1)/5)+1
790 b(j*2+2)=a-5*(b(j*2+1)-1)
800 NEXT j
810 FOR j=0 TO t
820 l=(b(j+1)-1)*5+b(j+t+2)
830 PRINT CHR$(a(l)+ca);
840 NEXT j
850 NEXT i
9999 REM end
```

ANALISIS. ¿QUE CIFRADO?

```
10 REM QUE CIFRADO?
15 MODE 1
16 CLS
20 PRINT "PROGRAMA DE ANALISIS 'QUE CIFR
ADO?"
30 LOCATE 3,3:PRINT "TEXTO";
40 INPUT t$
45 IF t$="0" THEN 9999
50 FOR i=1 TO LEN(t$)
60 IF i>LEN(t$) THEN 130
70 IF MID$(t$,i,1)>="a" AND MID$(t$,i,1)
<="z" THEN 130
80 r$=""
90 IF i>1 THEN r$=LEFT$(t$,i-1)
100 IF i<LEN(t$) THEN r$=r$+MID$(t$,i+1,
LEN(t$))
110 t$=r$
120 GOTO 60
130 NEXT i
140 lt=LEN(t$)
150 IF lt>25 THEN 180
160 LOCATE 1,3:PRINT "?"
170 GOTO 30
180 ca=ASC("a")-1
190 DIM f(27)
200 FOR i=1 TO lt
210 f(ASC(MID$(t$,i,1))-ca)=f(ASC(MID$(t
$,i,1))-ca)+1
220 NEXT i
230 m=0
235 ol=0
240 FOR i=1 TO 26
250 IF f(i)>m THEN m=f(i)
255 IF f(i)=0 THEN ol=1
260 NEXT i
270 CLS
290 LOCATE 5,1:PRINT "abcdefghijklmnopqr
stuvwxyz"
300 PLOT 70,27.43
310 DRAWR 410,0
320 PLOT 70,27.43
330 DRAWR 0,350
340 PLOT 70,27.43
350 LOCATE 1,2:PRINT "20%":LOCATE 1,7:PR
INT "15%":LOCATE 1,12.6:PRINT "10%":LOCA
TE 1,19:PRINT "5%"
370 FOR i=1 TO 27
373 h=f(i)/lt
377 IF h>0.2 THEN h=0.2
380 DRAWR 15,1.7*(12+h*810-YPOS)
390 NEXT i
400 IF INKEY$="" THEN 400
410 CLS
420 s=0
430 FOR i=1 TO 26
440 s=s+f(i)*(f(i)-1)
450 NEXT i
460 ic=s/(lt*(lt-1))
470 PRINT "INDICE DE COINCIDENCIA DE LET
RAS AISLADAS=";ic
480 DIM p(702)
490 ll=lt
500 IF ll/2>INT(ll/2) THEN ll=ll-1
510 FOR i=1 TO ll STEP 2
520 p=(ASC(MID$(t$,i,1))-ca)*26+ASC(MID$
(t$,i+1,1))-ca
530 p(p)=p(p)+1
540 NEXT i
550 s=0
560 FOR i=1 TO 676
570 s=s+p(i)*(p(i)-1)
580 NEXT i
590 ip=s/(ll*(ll-1))
600 PRINT:PRINT:PRINT "INCIDENCIA DE COI
NCIDENCIA DE PARES DE LETRAS";ip
9999 REM fin
```

ANALISIS GRONSFELD

```
10 REM ANALISIS GRONSFELD
14 DIM f$(255),d(255)
15 DIM e(26),t(26,26),c(26),w(20),o(25),
p(25,10),k(25)
16 MODE 1:CLS
20 LOCATE 9,12:PRINT "PONGA LA CINTA CON
 DATOS":LOCATE 8,13:PRINT "PULSE LUEGO C
UALQUIER TECLA"
```

```
30 SOUND 1,239,100
40 CALL &BB18
46 'SI FUESE DISCO PONGASE "!DISC" EN 50
50 !TAPE
51 OPENIN "frec"
52 FOR i=1 TO 26
53 INPUT #9,e(i)
54 NEXT
55 CLOSEIN
56 OPENIN "trans"
57 FOR i=1 TO 26
58 FOR j=1 TO 26
59 INPUT #9,t(i,j)
60 NEXT:NEXT
61 CLOSEIN
70 CLS
80 PRINT "PROGRAMA DE ANALISIS GRONSFELD
90 LOCATE 3,3:PRINT "TEXTO";
100 INPUT t$
105 IF t$="0" THEN 9999
110 FOR i=1 TO LEN(t$)
120 IF i>LEN(t$) THEN 190
130 IF MID$(t$,i,1)>="a" AND MID$(t$,i,1
)<="z" THEN 190
140 r$=""
150 IF i>1 THEN r$=LEFT$(t$,i-1)
160 IF i<LEN(t$) THEN r$=r$+RIGHT$(t$,LE
N(t$)-i)
170 t$=r$
180 GOTO 120
190 NEXT i
210 lt=LEN(t$)
220 IF lt>10 THEN 250
230 LOCATE 1,3:PRINT "?"
240 GOTO 90
250 CLS:LOCATE 1,1:PRINT "TEXTO: ";t$
255 ca=ASC("a")-1
260 FOR qw=1 TO lt:f$(qw)=" ":d(qw)=1:NE
XT qw
280 nr=0
290 CLS
295 PRINT "FACTORES DE REPETICION:"
300 GOSUB 5000
430 PRINT "HAY";nr;"REPETICIONES"
740 FOR i=1 TO lt
750 l=ASC(MID$(t$,i,1))-ca
760 c(l)=c(l)+1
770 NEXT i
780 s=0
790 FOR i=1 TO 26
800 s=s+c(i)*(c(i)-1)
810 NEXT i
820 ic=s/(lt*(lt-1))
830 PRINT:PRINT "INDICE DE COINCIDENCIA
:";ic
840 PRINT:INPUT "Longitud de palabra cla
ve a buscar";kl
845 CLS
850 IF kl=0 THEN GOTO 9999
860 IF kl<2 OR kl>lt/2 OR kl>INT(kl) THE
N 840
920 PRINT:PRINT "LONGITUD DE LA CLAVE :
";kl
930 FOR qw=1 TO 25:k(qw)=0:FOR wq=1 TO 1
0:p(qw,wq)=0:NEXT wq:NEXT qw
931 FOR qw=1 TO lt:f$(qw)=" ":NEXT qw
935 FOR i=1 TO kl:k(i)=-1:NEXT i
940 FOR i=1 TO 26
950 c(i)=c(i)/lt
960 NEXT i
961 LOCATE 1,25:PRINT "PULSE CUALQUIER T
ECLA."
962 r$=INKEY$
963 IF r$="" THEN 962
965 CLS
969 GOTO 7000
970 FOR c=1 TO kl
980 GOSUB 8000
990 NEXT c
1140 nc=0
1150 nc=nc+1
1160 IF lt/(nc*kl)>15 THEN 1150
1165 cl=nc*kl
1167 nr=lt/cl
1260 GOSUB 8200
1270 LOCATE 1,24:PRINT "PULSE a,b,c,d,e,
f,k,n,p,s,t,w o 0."
1280 r$=INKEY$
1290 IF r$="" THEN 1280
1300 LOCATE 1,24:PRINT TAB (39);" "
1305 IF r$="a" THEN 7000
1310 IF r$<>"b" THEN 1380
1320 GOSUB 8300
1330 k(c)=-1
1333 FOR i=1 TO 10
1335 p(c,i)=0
1337 NEXT i
1340 FOR i=c TO lt STEP kl
1350 f$(i)=" "
1360 NEXT i
1370 GOTO 1260
1380 IF r$<>"c" THEN 1410
1400 GOTO 1270
1410 IF r$<>"d" THEN 1450
1420 FOR qw=1 TO lt:f$(qw)=" ":NEXT qw
1430 FOR i=1 TO kl
1431 k(i)=-1
1432 NEXT i
1435 FOR qw=1 TO 25:FOR wq=1 TO 10:p(qw,
wq)=0:NEXT wq:NEXT qw
1440 GOTO 1260
1450 IF r$<>"e" THEN 1500
1460 GOSUB 9000:INPUT "Letra";l$
1465 IF l$="0" THEN 9999
1470 IF LEN(l$)<>1 OR l$<"a" OR l$>"z" T
HEN 1460
1480 LOCATE 1,22:PRINT TAB(40);
1485 LOCATE 1,22:PRINT l$;":";e(ASC(l$)-
ca)
1490 GOTO 1270
1500 IF r$<>"f" THEN 1550
1505 z=2
1510 FOR c=1 TO kl
1520 IF k(c)<0 THEN IF (f$(kl+c-1)<>" ")
 OR (f$(c+1)<>" ") THEN GOSUB 8000:GOSUB
 8200
1530 NEXT c
1533 z=z-1
1536 IF z>=0 THEN 1510
1537 FOR i=1 TO kl
1538 IF k(i)<0 THEN 1505
1539 NEXT i
```

```
1540 GOTO 1260
1550 IF r$<>"k" THEN GOTO 1580
1560 CLS
1570 GOTO 840
1580 IF r$<>"n" THEN 1620
1590 GOSUB 8300
1600 GOSUB 8000
1610 GOTO 1260
1620 IF r$="p" THEN 7230
1625 IF r$<>"s" THEN 1660
1630 CLS
1631 GOSUB 9000:PRINT "CLAVE : ";
1632 FOR i=1 TO kl
1633 PRINT k(i);
1634 NEXT i
1640 PRINT:PRINT:FOR i=1 TO lt:PRINT f$(
i);:NEXT i:PRINT
1650 GOTO 9999
1660 IF r$<>"t" THEN 1740
1665 GOSUB 9000
1670 INPUT "Letras";l$
1675 IF l$="0" THEN THEN 9999
1680 IF LEN(l$)<>2 THEN 1670
1690 l1=ASC(LEFT$(l$,1))-ca
1700 l2=ASC(RIGHT$(l$,1))-ca
1710 IF l1<1 OR l1>26 OR l2<1 OR l2>26 T
HEN 1665
1720 LOCATE 15,22:PRINT l$;":";t(l1,l2)
1730 GOTO 1270
1740 IF r$<>"w" THEN 1800
1750 GOSUB 8300
1755 GOSUB 9000
1760 INPUT "Clave";d
1770 IF d<0 OR d>9 OR d>INT(d) THEN 1760
1780 GOSUB 8170
1790 GOTO 1260
1800 IF r$="0" THEN 9999
1810 LOCATE 1,25:PRINT "?"
1820 SOUND 1,478,100
1830 GOTO 1270
1840 ERASE w,o
5000 FOR i=2 TO 6
5010 FOR k=1 TO lt-2*i+1
5020 FOR j=i+k TO lt-i+1
5030 IF MID$(t$,k,i)=MID$(t$,j,i) THEN G
OSUB 6000
5040 NEXT j:NEXT k:NEXT i
5050 RETURN
6000 d=j-k
6005 nr=nr+1
6010 PRINT STR$(nr);".";STR$(k);",";j;MI
D$(t$,k,i);" DIST=";d;"DIV";
6030 w=d:IF d>10 THEN w=10
6040 FOR dv=2 TO w
6050 IF d/dv=INT(d/dv) THEN PRINT "-";dv
;
6060 NEXT dv
6070 PRINT:RETURN
7000 LOCATE 1,24:INPUT "Palabra probable
";w$
7010 IF w$="0" THEN 9999
7020 IF w$="" THEN 970
7030 lw=LEN(w$)
7040 FOR qw=1 TO 25:o(qw)=0:NEXT qw
7050 FOR i=1 TO lw
7060 w(i)=ASC(MID$(w$,i,1))-ca
7065 IF w(i)<1 OR w(i)>26 THEN 7000
7070 NEXT i
7080 np=0
7100 FOR i=0 TO lt-lw-1
7110 FOR j=1 TO lw
7120 l=ASC(MID$(t$,i+j,1))-ca
7130 FOR k=0 TO 9
7140 n=l-k
7150 IF n<1 THEN n=n+26
7160 IF n=w(j) THEN 7190
7170 NEXT k
7180 GOTO 7220
7190 NEXT j
7200 np=np+1
7210 o(np)=i+1
7220 NEXT i
7230 CLS
7235 IF np>0 THEN 7260
7240 PRINT:PRINT "<";w$;"> NO PUEDE SER.
"
7250 GOTO 7000
7260 PRINT:PRINT "PUEDE ESTAR EN";np;"SI
TIOS"
7270 FOR i=1 TO np
7280 PAPER 4:PEN 2:PRINT i;". CARACTER "
;o(i);"-";
7290 PRINT MID$(t$,o(i),lw)
7330 NEXT i
7335 PRINT:PRINT
7340 PRINT:INPUT "Numero de la opcion qu
e escoge";o
7345 IF o=0 THEN 9999
7350 IF o<1 OR o>np OR o>INT(o) THEN 734
0
7360 p=o(o)
7370 c=p-kl*INT(p/kl)
7380 IF c=0 THEN c=kl
7390 FOR j=0 TO lw-1
7400 l=ASC(MID$(t$,p+j,1))-ca
7410 FOR k=0 TO 9
7420 n=l-k
7430 IF n<1 THEN n=n+26
7440 IF n<>w(j+1) THEN NEXT k
7450 d=k
7455 GOSUB 8170
7460 c=c+1
7470 IF c>kl THEN c=c-kl
7480 NEXT j
7490 CLS
7500 GOTO 1140
8000 b=999
8005 d=0
8010 FOR k=0 TO 9
8020 IF p(c,k+1)<>0 THEN 8160
8030 t=0
8040 n=l-k
8050 IF n<1 THEN n=n+26
8060 t=t+(lt/kl)*ABS(e(n)-c(l))
8065 FOR j=0 TO lt-kl STEP kl
8070 p=c+j
8080 l=ASC(MID$(t$,p,1))-ca
8100 IF p>1 THEN IF f$(p+1)<>" " THEN t=
t-t(ASC(f$(p-1))-ca,n)
8110 IF p<l AND f$(p+1)<>" " THEN t=t-t(
n,ASC(f$(p+1))-ca)
8120 NEXT j
```

```
8130 IF t>b THEN 8160
8140 b=t
8150 d=k
8160 NEXT k
8170 k(c)=d
8175 p(c,d+1)=1
8180 FOR i=c TO lt STEP kl
8182 l=ASC(MID$(t$,i,1))-ca-d
8184 IF l<1 THEN l=l+26
8186 f$(i)=CHR$(l+ca)
8188 NEXT i
8190 RETURN
8200 LOCATE 7,1:FOR i=1 TO kl:PRINT RIGH
T$(STR$(i),1);:NEXT i
8201 LOCATE 7,4
8205 FOR i=0 TO nr-1
8210 PRINT TAB(7);
8215 FOR qw=cl*i+1 TO cl*(i+1):PRINT f$(
qw);:NEXT qw:PRINT
8220 NEXT i
8225 IF lt/cl>INT(lt/cl) THEN LOCATE 7,i
+4:FOR qw=cl*i+1 TO lt:PRINT f$(qw);:NEX
T qw:PRINT
8226 LOCATE 1,2
8230 PRINT "CLAVE=";
8240 FOR j=1 TO kl
8250 PRINT MID$(STR$(k(j)),2,1);
8260 NEXT j
8265 PRINT ff$
8270 PRINT
8280 RETURN
8300 GOSUB 9000:INPUT "Que columna";c
8310 IF c=0 THEN 9999
8320 IF c<1 OR c>kl OR c>INT(c) THEN 830
0
8330 RETURN
9000 LOCATE 1,22:PRINT SPACE$(74):LOCATE
 1,22:RETURN
9999 REM fin
```

SEGURO

```
10 REM SEGURO
15 MODE 1
16 CLS
20 PRINT "PROGRAMA DE CIFRADO 'SEGURO'"
30 LOCATE 3,3:PRINT "MODO";
40 INPUT m$
50 IF m$="0" THEN 9999
60 IF m$="c" OR m$="d" THEN 90
70 LOCATE 1,3:PRINT "?"
80 GOTO 30
90 LOCATE 1,3:PRINT " MODO : ";m$
100 LOCATE 3,5:PRINT "NUMERO CLAVE : ";
110 INPUT k
120 IF k=0 THEN 9999
130 IF k>0 AND k<65536 AND k=INT(k) THEN
 160
140 LOCATE 1,5:PRINT "?"
150 GOTO 100
160 LOCATE 3,5:PRINT "NUMERO CLAVE : ";k
170 LOCATE 3,7:PRINT "PALABRA CLAVE : ";
180 INPUT k$
190 IF k$="0" THEN 9999
200 lk=LEN(k$)
210 IF lk>0 THEN 240
220 LOCATE 1,7:PRINT "?"
230 GOTO 170
240 DIM a(25)
250 DIM l(25)
260 ca=ASC("a")-1
270 a=0
280 FOR i=1 TO lk
290 c=ASC(MID$(k$,i,1))-ca
300 IF c<1 OR c>25 THEN 220
310 IF l(c)>0 THEN 350
320 a=a+1
330 a(a)=c
340 l(c)=a
350 NEXT i
360 FOR i=1 TO 25
370 IF l(i)>0 THEN 410
380 a=a+1
390 a(a)=i
400 l(i)=a
410 NEXT i
415 LOCATE 1,7:PRINT TAB(40)
420 LOCATE 3,7:PRINT "ALFABETO ALTERADO
:"
430 FOR i=0 TO 4
440 FOR j=1 TO 5
450 LOCATE 21+j,7+i:PRINT CHR$(a(i*5+j)+
ca)
460 NEXT j
470 NEXT i
480 LOCATE 3,13:PRINT "TEXTO";
490 INPUT t$
500 IF t$="0" THEN 9999
510 FOR i=1 TO LEN(t$)
520 IF i>LEN(t$) THEN 590
530 IF MID$(t$,i,1)>="a" AND MID$(t$,i,1
)<="z" THEN 590
540 r$=""
550 IF i>1 THEN r$=LEFT$(t$,i-1)
560 IF i<LEN(t$) THEN r$=r$+RIGHT$(t$,LE
N(t$)-i)
570 t$=r$
580 GOTO 520
590 NEXT i
600 lt=LEN(t$)
610 IF lt>0 THEN 640
620 LOCATE 1,13:PRINT "?"
630 GOTO 490
640 LOCATE 3,13:PRINT "TEXTO : ";t$:PRIN
T:PRINT
645 RANDOMIZE k
646 IF m$="c" THEN PRINT:PRINT "Texto ci
frado: ";
```

```
647 IF m$="d" THEN PRINT:PRINT "Texto de
scifrado:";
648 DIM tm$(lt)
649 w=RND(-k):w=0
650 FOR m=1 TO lt
651 tm$(m)=MID$(t$,m,1)
652 NEXT m
660 IF m$="d" THEN 760
670 FOR i=1 TO lt
680 c=ASC(tm$(i))-ca
690 x=INT((c-1)/5)+INT(5*RND)+2
700 IF x>5 THEN x=x-5
710 y=c-INT((c-1)/5)*5+INT(5*RND)+1
720 IF y>5 THEN y=y-5
730 PRINT CHR$(1((x-1)*5+y)+ca);
740 NEXT i
750 GOTO 9999
760 FOR i=1 TO lt
770 c=a(ASC(tm$(i))-ca)
780 x=INT((c-1)/5)-INT(5*RND)
790 IF x<1 THEN x=x+5
800 y=c-INT((c-1)/5)*5-INT(5*RND)-1
810 IF y<1 THEN y=y+5
820 PRINT CHR$((x-1)*5+y+ca);
830 NEXT i
9999 REM fin
```

CREACION DE DATOS

```
10 REM PROGRAMA DE CREACION DE DATOS
20 MODE 1:CLS
30 PRINT "PROGRAMA DE CREACION DE DATOS"
40 LOCATE 1,3:PRINT "ESCRIBA LA FREQUENC
IA PARA CADA LETRA   SEGUN SE PIDA"
50 DIM e(26)
60 FOR i=1 TO 26
70 PRINT CHR$(96+i);"? ";
80 INPUT e(i)
90 NEXT i
100 CLS
110 LOCATE 1,1:PRINT "ESCRIBA AHORA LOS
DATOS DE TRANSICION   PARA CADA PAR DE L
ETRAS"
120 DIM t(26,26)
130 FOR i=1 TO 26
140 FOR j=1 TO 26
150 PRINT CHR$(96+i);CHR$(96+j);"? ";
160 INPUT t(i,j)
170 NEXT j
180 NEXT i
190 CLS
200 LOCATE 1,7:PRINT "INTRODUZCA LA CINT
A PARA ALMACENAR LOS DATOS,Y PULSE LUEGO
 CUALQUIER LETRA."
210 ERASE e,t
220 DIM e(26)
230 DIM t(26,26)
240 IF INKEY$="" THEN 240
250 |TAPE
260 'SI FUERA PARA DISCO INTRODUCIR "|DI
SC" EN 250
270 OPENOUT "frec"
280 FOR i=1 TO 26
290 WRITE #9,e(i)
300 NEXT
310 CLOSEOUT
320 OPENOUT "trans"
330 FOR i=1 TO 26
340 FOR j=1 TO 26
350 WRITE #9,t(i,j)
360 NEXT:NEXT
370 CLOSEOUT
9999 'fin
```

Programas para Commodore

Nota.—A lo largo de los listados, para mayor claridad, se indica el espacio con {SPC} y un conjunto de espacios con el símbolo anterior y un número. Por ejemplo, {SPC 5} indica la inclusión de cinco espacios en blanco.

CESAR

```
10 REM              CESAR
15 POKE53280,0: POKE 53281,0: POKE646,5
20 PRINT CHR$(147): REM BORRA PANTALLA
25 PRINT CHR$(18);
   "{SPC6}PROGRAMA{SPC}DE{SPC}CIFRADO{SP
C}";
26 PRINT CHR$(34);"CESAR";CHR$(34);
   "{SPC6}"
30 POKE 214,4: PRINT
35 LL$="": FOR N=0 TO 38: LL$=LL$+"{SPC}
":     NEXT
40 PRINT "{SPC3}MODO{SPC}Y{SPC}CLAVE";
50 INPUT M$
60 A$=LEFT$(M$,1)
70 IF A$="0" THEN 9999
75 IF A$<"C" OR A$>"D" THEN 100
80 B$=MID$(M$,2,1)
85 IF B$<"A" OR B$>"Z" THEN 100
90 GOTO 120
100 POKE 214,4: PRINT: PRINT LL$
102 POKE 214,4: PRINT
105 PRINT"{SPC3}???";
110 GOTO 40
120 POKE 214,4: PRINT: PRINT LL$
125 POKE 214,4: PRINT
127 PRINT "{SPC}MODO{SPC}:{SPC}";A$;TAB(
20);              "CLAVE{SPC}:{SPC}";B$
130 K=ASC(B$)-65
140 POKE 214,6: PRINT
145 PRINT"{SPC}TEXTO{SPC}:{SPC}";
150 INPUT T$
160 IF LEFT$(T$,1)="0" THEN 9999
170 IF A$="C" THEN 190
180 K=-K
```

```
190 L=LEN(T$)
195 POKE 214,12: PRINT: PRINT TAB(11);
200 FOR I=1 TO L
210 C$=MID$(T$,I,1)
220 IF "A"<=C$ AND "Z">=C$ THEN 250
230 PRINT"{SPC}";
240 GOTO 280
250 W=ASC(C$)-65+K
260 GOSUB 420
270 PRINTCHR$(W+65);
280 NEXT I
285 FOR I=1 TO 2000: NEXT
290 IF A$="C" THEN 9999
295 N=5: POKE 198,0
300 GOSUB 600
320 GET R$
330 IF R$="S" THEN 380
340 IF R$="N" THEN POKE646,7: GOTO 9999
350 N=N+.05: IF N>=16 THEN N=1
355 POKE 646,N
360 GOTO300
380 W=1-K
385 POKE646,0: GOSUB 600: POKE646,5
390 GOSUB 420
400 K=-W
410 GOTO 195
420 IF W<=25 THEN 440
430 W=W-26
435 RETURN
440 IF W>=0 THEN RETURN
450 W=W+26
460 RETURN
600 POKE 214,20: PRINT
610 PRINT TAB(5);CHR$(18);
    "{SPC3}DESEA{SPC}CONTINUAR{SPC3}(S/N
){SPC}?{SPC3}"
620 RETURN
9999 END
```

MONO

```
10 REM   CIFRADO MONOALFABETICO
15 GOSUB 8300: REM INICIALIZACION
20 POKE 214,10: PRINT: PRINT "{SPC}BUSQU
E{SPC}EN{SPC}LA{SPC}CINTA{SPC}EL{SPC}FIC
HERO{SPC}DE{SPC}DATOS,"
25 PRINT: PRINT "{SPC2}DESPUES{SPC}PULSE
{SPC}CUALQUIER{SPC}TECLA."
30 GOSUB 8400
40 POKE 198,0: WAIT 198,1
45 POKE 198,0
50 DIM E(26): GOSUB 8500:
   REM LEE LA TABLA DE FRECUENCIAS
60 DIM T(26,26): GOSUB 8600:
   REM LEE LA TABLA DE TRANSICIONES
65 DIM C(26),N(26)
70 PRINT CHR$(147)
80 PRINT CHR$(18);"{SPC3}PROGRAMA{SPC}DE
{SPC}CIFRADO{SPC}MONOALFABETICO.{SPC2}";
CHR$(146)
90 POKE 214,2: PRINT:
   PRINT "{SPC3}TEXTO{SPC}:";
100 INPUT T$
110 IF T$="0" THEN 9999
120 LT=LEN(T$)
130 IF LT<=9 THEN GOSUB 8400: GOTO 70
160 T1$=""
165 FOR I=1 TO LT
170 X1$=MID$(T$,I,1)
175 IF X1$<"A" OR X1$>"Z" THEN X1$="{SPC
}"
177 T1$=T1$+X1$
180 NEXT
185 T$=T1$
190 POKE 214,2:PRINT:
    PRINT "{SPC3}TEXTO{SPC}:{SPC3}";T$
200 BL=6+INT((LT-1)/15)
210 FOR JJ=1 TO 26: C(JJ)=0: NEXT JJ
220 CA=64
230 FOR I=1 TO LT
240 X1$=MID$(T$,I,1)
245 IF X1$<>"{SPC}"  THEN C(ASC(X1$)-CA)
=       C(ASC(X1$)-CA)+1/LT
250 NEXT I
260 GOSUB 8000
265 PRINT CHR$(147)
270 FOR I=1 TO 26
280 PRINT CHR$(18);CHR$(150);"{SPC}";
        CHR$(I+CA);"{SPC}:";CHR$(159);
285 PRINT LEFT$(STR$(C(I))+"{SPC5}",5),
290 NEXT I
300 GOSUB 8000
310 A$="**************************"
315 B$=A$
320 PRINT CHR$(147);CHR$(142);CHR$(207);
325 FOR N=1 TO 38
330 PRINT CHR$(183);
335 NEXT N
340 PRINT CHR$(208);
345 FOR N=1 TO 4
350 PRINT CHR$(180);SPC(38);CHR$(170);
355 NEXT N
360 PRINT CHR$(204);
365 FOR N=1 TO 38
370 PRINT CHR$(175);
375 NEXT N
380 PRINT CHR$(186)
385 PRINT CHR$(19);CHR$(17);CHR$(17);
    TAB(8);"ABCDEFGHIJKLMNOPQRSTUVWXYZ"
390 PRINT TAB(8);A$: P$=""
392 PRINT: PRINT: PRINT
395 FOR I=0 TO 15*INT((LT-1)/15) STEP 15
400 J=15
410 IF I+J>LT THEN J=LT-I
420 PRINT TAB(3);MID$(T$,I+1,J);
  TAB(22);
430 FOR N=1 TO J
```

```
440 C$="{SPC}"
450 IF MID$(T$,I+N,1)<>"{SPC}" THEN
      C$=MID$(A$,ASC(MID$(T$,I+N,1))-C
A,1)
460 P$=P$+C$
470 PRINTC$;
480 NEXT N
485 PRINT
490 NEXT I
500 POKE214,21:PRINT: PRINT  CHR$(18);
    "{SPC4}PULSE{SPC}B,C,D,E,F,N,P,S,T,0
{SPC4}"
505 POKE 198,0
510 GET R$
520 IF R$="" THEN 510
530 FORQ=1584 TO 1943:POKEQ,32:NEXT
535 IF R$="N"  THEN 310
540 IF R$<>"B" THEN 920
560 GOSUB 8200
570 PRINT CHR$(18);CHR$(150);"{SPC}";
      CHR$(L+CA);"{SPC}:";CHR$(159);
575 PRINT "FRECUENCIA{SPC}:";LEFT$(STR$(
990 IF R$<>"E" THEN 1040
1010 GOSUB 8200
1020 PRINT TAB(1);L$;":{SPC}";E(L)
1030 GOTO 500
1040 IF R$<>"F" THEN 1090
1060 GOSUB 8200
1070 PRINT TAB(1);L$;":{SPC}";C(L)
1080 GOTO 500
1090 IF R$="N" THEN 310
1100 IF R$<>"P" THEN 1200
1120 POKE211,1:POKE214,18:SYS58640:INPUT
 "LETRAS";L$
1130 IF L$="0" THEN 9999
1140 IF LEN(L$)<>2 THEN 1120
1150 L1=ASC(LEFT$(L$,1) )-CA
1160 L2=ASC(RIGHT$(L$,1))-CA
1170 IF L1<1 OR L1>26 OR L2<1 OR L2>26
    THEN 1120
1180 PRINT TAB(1);L$;":{SPC}";T(L1,L2)
1190 GOTO 500
1200 IF R$<>"S" THEN 1240
1210 FOR I=4 TO 21
1212 POKE 214,I: PRINT: PRINTTAB(38); "{
SPC}"
1217 NEXT I
1220 POKE 214,4: PRINT: PRINT P$
1230 GOTO 9999
1240 IF R$<>"T" THEN 1340
1250 GOSUB 8200
1260 Q$=L$
1270 LL=L
1280 GOSUB8200
1300 IF MID$(B$,L,1)<>"*" THEN 1280
1310 IF MID$(A$,LL,1)="*" THEN 1320
1315 J=ASC(MID$(A$,LL,1))-CA:
     B$=LEFT$(B$,J-1)+"*"+MID$(B$,J+1)
1320 A$=LEFT$(A$,LL-1)+L$+MID$(A$,LL+1)
1325 B$=LEFT$(B$,L-1)+Q$+MID$(B$,L+1)
1330 GOTO320
1340 IF R$="0" THEN 9999
1350 POKE214,21: PRINT: PRINT"?"
1360 GOSUB 8400
1370 GOTO 500
8000 POKE214,21: PRINT
8005 PRINT CHR$(18);"{SPC10}PULSE{SPC}CU
ALQUIER{SPC}TECLA{SPC9}";CHR$(146)
8010 POKE 198,0
8015 GET R$
8020 IF R$="" THEN 8015
8030 IF R$="0" THEN 9999
8040 RETURN
8200 POKE211,1:POKE214,18:SYS58640:PRINT
 "LETRA{SPC}?";: POKE 198,0
8205 GET L$: IF L$="" THEN 8205
8210 IF L$="0" THEN 9999
8220 IF L$<"A" OR L$>"Z" THEN 8205
8230 PRINT L$: L=ASC(L$)-CA
8250 RETURN
8300 REM INICIALIZACION
8310 FOR N=54272 TO 54296
8320 POKE N,0
8330 NEXT N
8360 POKE 54296,15
8370 POKE 53280,8: POKE53281,9
8380 PRINT CHR$(153);CHR$(147);
     CHR$(14)
8390 RETURN
8400 REM TOCA UNA NOTA
8410 POKE 54276,0
8420 POKE 54277,144: POKE 54278,0
8430 S9=RND(1)*256
8440 POKE 54272,S9
8450 POKE 54273,255-S9
8460 POKE 54276,17
8470 RETURN
8500 OPEN 1,1,0,"FRECUENCIAS"
8510 FOR N=1 TO 26
8520 INPUT#1,E(N)
8530 NEXT
8540 CLOSE1
8550 RETURN
8600 OPEN 1,1,0,"TRANSICIONES"
8610 FOR N=1 TO 26
8620 FOR I=1 TO 26
8630 INPUT#1,T(N,I)
8640 NEXT I,N
8650 CLOSE1
8660 RETURN
9999 END
```

PROGRAMA DE ANALISIS DE FRECUENCIAS

```
10 REM PROGRAMA DE ANALISIS FRECUENCIAL
15 DEF FN N(X)=ASC(MID$(T$,X,1))-CA
16 POKE 53281,9: POKE 53280,9
20 PRINT CHR$(147);CHR$(18);"{SPC2}PROGR
AMA{SPC}DE{SPC}ANALISIS{SPC}DE{SPC}FRECU
ENCIAS{SPC2}"
30 X=0: Y=2: GOSUB 2000
40 INPUT"TEXTO:";T$
45 FORQ=1104TO1223:POKEQ,32:NEXTQ
50 IF T$="0" THEN 9999
60 FOR I=1 TO LEN (T$)
70 IF I>LEN (T$) THEN 140
80 IF MID$(T$,I,1)>="A" AND
   MID$(T$,I,1)<="Z" THEN 140
90 R$=""
100 IF I>1 THEN R$=LEFT$(T$,I-1)
110 IF I<LEN(T$) THEN R$=R$+MID$(T$,I+1)
120 T$=R$
130 GOTO 70
140 NEXT I
150 LT=LEN(T$)
160 IF LT>3 THEN 190
170 X=0: Y=2: GOSUB 2000
180 GOTO 40
190 X=0: Y=2: GOSUB 2000:PRINT "TEXTO{SP
C}:";T$
200 GOSUB 8000
210 CA=64: REM VALOR ASCII DE "A"-1
220 DIM E(26)
230 PRINT "FRECUENCIA{SPC}RELATIVA{SPC}D
E{SPC}LAS{SPC}LETRAS{SPC}:": PRINT
240 FOR I=1 TO LT
245 N=FN N(I)
250 E(N)=E(N)+1
260 NEXT I
270 FOR I=1 TO 26
280 PRINT CHR$(18); CHR$(5); CHR$(I+CA);
    CHR$(158);":{SPC}";:AA=E(I)/LT:GOSUB
3000
290 NEXT I
300 GOSUB 8000
310 DIM D(26)
320 FOR I=1 TO LT-1
330 IF MID$(T$,I,1) <> MID$(T$,I+1,1)
    THEN 340
335 N=FN N(I): D(N)=D(N)+1
340 NEXT I
350 PRINT "LETRAS{SPC}REPETIDAS{SPC}:":
PRINT
360 FOR I=1 TO 26
370 PRINT CHR$(18); CHR$(5); CHR$(I+CA);
    CHR$(158); ":{SPC}";:AA=D(I): GOSUB
3000
380 NEXT I
390 GOSUB 8000
400 PRINT "FRECUENCIA{SPC}DE{SPC}DOS{SPC
}LETRAS{SPC}CONSECUTIVAS{SPC}:": PRINT
410 DIM T(26,26)
420 FOR I=1 TO LT-1
430 N=FN N(I): J=FN N(I+1)
435 T(N,J)=T(N,J)+1
440 NEXT I
450 FOR I=1 TO 26
460 FOR J=1 TO 26
470 IF T(I,J)<=0 THEN 480
475 PRINT CHR$(18);CHR$(5); CHR$(I+CA);
476 PRINT CHR$(J+CA);CHR$(158); ":{SPC}"
;:      AA=T(I,J): GOSUB 3000
480 IF PEEK(214)>=20 AND PEEK(653)=1
    THEN GOSUB 8000
485 REM PULSANDO SHIFT SE DETIENE EL
    PROCESO SI SE LLENA LA PANTALLA
490 NEXT J,I
510 GOSUB 8000
515 DIM F(26,26)
520 PRINT "LETRAS{SPC}EN{SPC}ORDEN{SPC}I
NVERSO{SPC}:":      PRINT
530 FOR I=1 TO 26
540 FOR J=1 TO 26
550 IF T(I,J)<=0 OR T(J,I)<=0 OR I=J OR
    F(I,J)<>0 OR F(J,I)<>0 THEN 560
555 PRINT CHR$(18);CHR$(5); CHR$(I+CA);
556 PRINT CHR$(J+CA); CHR$(158); ":{SPC}
";:      AA=T(I,J): GOSUB 3000
557 PRINT CHR$(18);CHR$(5); CHR$(J+CA);
558 PRINT CHR$(I+CA); CHR$(158); ":{SPC}
";:      AA=T(J,I): GOSUB 3000
559 F(I,J)=1
560 IF PEEK(214)>=20 AND PEEK(653)=1
    THEN GOSUB 8000
565 REM PULSANDO SHIFT SE DETIENE EL
    PROCESO SI SE LLENA LA PANTALLA
570 NEXT J,I
590 GOSUB 8000
600 DIM R(26,26)
610 FOR I=1 TO 26
620 IF E(I)=0 THEN 660
630 FOR J=1 TO 26
640 R(I,J)=T(I,J)/E(I)
650 NEXT J
660 NEXT I
670 PRINT"PROBABILIDAD{SPC}DE{SPC}CONTAC
TOS{SPC}LADO{SPC}DERECHO{SPC}:"
675 PRINT
680 FOR I=1 TO 26
690 FOR J=1 TO 26
700 IF R(I,J)<=0 THEN 710
705 PRINT CHR$(18);CHR$(5); CHR$(I+CA);
706 PRINT CHR$(J+CA);CHR$(158); ":{SPC}"
;:      AA=R(I,J): GOSUB 3000
710 IF PEEK(214)>=20 AND PEEK(653)=1
    THEN GOSUB 8000
715 REM PULSANDO SHIFT SE DETIENE EL
    PROCESO SI SE LLENA LA PANTALLA
720 NEXT J,I
740 GOSUB 8000
```

```
750 DIM L(26,26)
760 FOR I=1 TO 26
770 IF E(I)=0 THEN 810
780 FOR J=1 TO 26
790 L(I,J)=T(J,I)/E(I)
800 NEXT J
810 NEXT I
820 PRINT"PROBABILIDAD{SPC}DE{SPC}CONTAC
TOS{SPC}LADO{SPC}IZQUIERDO": PRINT
830 FOR I=1 TO 26
840 FOR J=1 TO 26
850 IF R(I,J)<=0 THEN 860
855 PRINT CHR$(18);CHR$(5); CHR$(J+CA);
856 PRINT CHR$(I+CA);CHR$(158); ":{SPC}"
;:      AA=L(I,J): GOSUB 3000
860 IF PEEK(214)>=20 AND PEEK(653)=1
    THEN GOSUB 8000
865 REM PULSANDO SHIFT SE DETIENE EL
    PROCESO SI SE LLENA LA PANTALLA
870 NEXT J,I
890 GOSUB 8000
900 DIM G(26,LT)
910 FOR I=1 TO 26
920 FOR J=2 TO LT-1
930 IF MID$(T$,J,1)=CHR$(I+CA) THEN
    G(I,J)=1
940 NEXT J
950 NEXT I
960 PRINT "GRUPOS{SPC}DE{SPC}TRES{SPC}LE
TRAS{SPC}CONSECUTIVAS{SPC}:":PRINT
970 FOR I=1 TO 26
980 IF E(I)=0 THEN 1050
985 R$=CHR$(I+CA)
986 IF E(I)=1 AND ( RIGHT$(T$,1)=R$ OR
    LEFT$(T$,1)=R$ ) THEN 1050
990 PRINT: PRINT CHR$(18); CHR$(5);
    CHR$(I+CA);
995 PRINT CHR$(158); ":{SPC}";
1000 FOR J=2 TO LT
1010 IFG(I,J)=1THENPRINTCHR$(150);CHR$(
     18);MID$(T$,J-1,3);CHR$(146);",";
1020 NEXT J
1030 PRINT CHR$(157);"{SPC}"
1040 IF PEEK(214)>=20 THEN GOSUB 8000
1050 NEXT I
1060 GOSUB 8000
1070 END
2000 POKE 214,Y-1: PRINT: PRINT TAB(X);:
     RETURN
3000 PRINT CHR$(159);LEFT$(STR$(AA)+
     "{SPC6}",6);CHR$(146),
3010 IF PEEK (211)=0 THEN PRINT
3020 RETURN
8000 X=10:Y=23: GOSUB 2000
8005 PRINT"PULSE{SPC}CUALQUIER{SPC}TECLA
"
8010 GET R$
8020 IF R$="" THEN 8010
8030 IF R$<>"C" THEN 8060
8040 PRINT:PRINT"PARA{SPC}SACAR{SPC}UNA{
SPC}COPIA{SPC}POR{SPC}IMPRESORA{SPC6}CON
SULTE{SPC}EL{SPC}APENDICE{SPC}FINAL."
8050 GOTO 8010
8060 IF R$="0" THEN 9999
8070 PRINT CHR$(147)
8080 RETURN
9999 END
```

AYUDA MONOALFABETICA

```
10 REM  *** MONOALFABETICO ***
15 POKE 53281,0: POKE 53280,0:POKE 646,5
20 PRINT CHR$(147);CHR$(18);"{SPC9}CIFRA
DO{SPC}MONOALFABETICO{SPC7}"
30 X=2: Y=X: GOSUB 2000
40 PRINT "{SPC2}MODO,{SPC}MEZCLA{SPC}Y{S
PC}CLAVE{SPC}:"
50 PRINT: INPUT M$
60 IF M$="0" THEN 9999
70 L=LEN(M$)
80 IF L<3 OR L>28 THEN 150
90 IF LEFT$(M$,1)<"C" OR LEFT$(M$,1)>"D"
   THEN I=1: GOTO 150
100 IF MID$(M$,2,1)<"S" OR
    MID$(M$,2,1)>"T" THEN I=2: GOTO 150
110 FOR I=3 TO L
120 IF MID$(M$,I,1)<"A" OR
       MID$(M$,I,1)>"Z" THEN 150
130 NEXT I
132 X=0: Y=8: GOSUB 2000
133 PRINT "{SPC}MODO{SPC3}={SPC}"; LEFT$
(M$,1);
134 PRINT "{SPC24}": PRINT
135 PRINT "{SPC}MEZCLA{SPC}={SPC}"; MID$
(M$,2,1):       PRINT
136 PRINT "{SPC}CLAVE{SPC2}={SPC}"; MID$
(M$,3)
140 GOTO 220
150 X=0: Y=8: GOSUB 2000:PRINT "ERROR{SP
C}";
160 IF L>28 THEN PRINT "MAS{SPC}DE{SPC}2
8{SPC}CARACTERES";: I=29: GOTO 200
170 IF I=1 THEN PRINT "EN{SPC}EL{SPC}MOD
O{SPC}(C/D)"
180 IF I=2 THEN PRINT
    "EN{SPC}LA{SPC}MEZCLA{SPC}(S/T)"
190 IF I>=3 THEN PRINT
    "EN{SPC}LA{SPC}CLAVE{SPC}(A-Z)"
200 X=0: Y=6: GOSUB 2000
205 PRINT TAB(I);"{SPC}^"
210 GOSUB 3000: GOTO 20
220 M$=M$+"ABCDEFGHIJKLMNOPQRSTUVWXYZ"
230 LA=LEN(M$)
240 C$=""
250 CA=64
260 DIM K$(26)
270 FOR I=3 TO LA
280 AS=ASC(MID$(M$,I,1))-CA
```

```
290 IF K$(AS)<>"" THEN 310
300 C$=C$+MID$(M$,I,1)
310 IF I<>L THEN 330
320 B=LEN(C$)
330 K$(AS)="*"
340 NEXT I
350 IF MID$(M$,2,1)="S" THEN 600
360 D=INT(26/B)
362 IF B*D=26 THEN 365
364 D=D+1
365 LC=B*D
390 IF LC<=26 THEN 430
400 FOR I=27 TO LC
410 C$=C$+"*"
420 NEXT I
430 DIM A$(B,D)
440 FOR I=1 TO B
450 FOR J=1 TO D
460 A$(I,J)=MID$(C$,(I-1)*D+J,1)
470 NEXT J
480 NEXT I
490 C$=""
500 FOR I=1 TO D
510 FOR J=B TO 1 STEP -1
520 IF A$(J,I)="*" THEN 540
530 C$=C$+A$(J,I)
540 NEXT J
550 NEXT I
600 X=0: Y=2: GOSUB 2000
605 FOR I=1 TO 39: PRINT"{SPC}";: NEXT I
606 PRINT: PRINT
608 FOR I=1 TO 39: PRINT"{SPC}";: NEXT I
610 X=0: Y=2: GOSUB 2000:
    PRINT "{SPC}TEXTO{SPC}:": PRINT
615 INPUT T$
620 X=0: Y=2: GOSUB 2000:
    PRINT "{SPC8)"
625 X=0: Y=6: GOSUB 2000
630 IF T$="0" THEN 9999
640 LT=LEN(T$)
650 IF LEFT$(M$,1)="C" THEN 725
660 DIM P$(26)
670 FOR I=1 TO 26
680 P$(ASC(MID$(C$,I,1))-CA)=CHR$(CA+I)
690 NEXT I
700 FOR I=1 TO 26
710 C$=LEFT$(C$,I-1)+P$(I)+MID$(C$,I+1)
720 NEXT I
725 PRINT "{SPC2)";CHR$(18);
730 FOR I=1 TO LT
740 IF MID$(T$,I,1)<"A" OR
       MID$(T$,I,1)>"Z" THEN 770
750 PRINTMID$(C$,ASC(MID$(T$,I,1))-CA,1)
;
760 GOTO 780
770 PRINT "{SPC)";
780 NEXT I
790 GOTO 9999
2000 POKE 214,Y-1: PRINT: PRINT TAB(X);:
     RETURN
3000 POKE 198,0
3010 X=10: Y=21: GOSUB 2000
3020 PRINT CHR$(18);"{SPC}PULSE{SPC}UNA{
SPC}TECLA{SPC}"
3030 GET RR$: IF RR$="" THEN 3030
3040 RETURN
9999 X=0:Y=22: GOSUB 2000: END
```

ZIG-ZAG

```
10 REM   ***   ZIG-ZAG   ***
15 POKE 53280,11: POKE53281,11: POKE 646
,3
20 PRINT CHR$(147)
25 PRINT TAB(5);CHR$(18);
   "PROGRAMA{SPC}DE{SPC}CIFRADO{SPC}'{SP
C}ZIG-ZAG{SPC}'
30{SPC}X=2:{SPC}Y=2:{SPC}GOSUB{SPC}2000
35{SPC}PRINT{SPC}"MODO Y CLAVE:":{SPC}PR
INT
40{SPC}INPUT{SPC}M$
50{SPC}IF{SPC}M$="0"{SPC}THEN{SPC}9999
60{SPC}IF{SPC}LEN(M$)<2{SPC}THEN{SPC}I=0
:{SPC}GOTO{SPC}110
70{SPC}M1$=LEFT$(M$,1)
75{SPC}IF{SPC}M1$<"C"{SPC}OR{SPC}M1$>"D"
{SPC}THEN{SPC}I=1:{SPC9}GOTO{SPC}110
80{SPC}FOR{SPC}I=2{SPC}TO{SPC}LEN(M$)
85{SPC}IF{SPC}VAL(MID$(M$,2,I))>9{SPC}TH
EN{SPC}110
90{SPC}NEXT{SPC}I
100{SPC}GOTO{SPC}130
110{SPC}X=0:{SPC}Y=8:{SPC}GOSUB{SPC}2000
:{SPC}PRINT"ERROR ";
112{SPC}IF{SPC}I>1{SPC}THEN{SPC}PRINT{SP
C23)"SOLO PUEDE SER UN NUMERO"
114{SPC}IF{SPC}I=1{SPC}THEN{SPC}PRINT{SP
C}"EN EL MODO (C/D)"
115{SPC}IF{SPC}I=0{SPC}THEN{SPC}PRINT{SP
C}"FALTA LA CLAVE":{SPC5}I=2
116{SPC}IF{SPC}I=-1{SPC}THEN{SPC}PRINT{S
PC}"EL NUMERO DEBE SER MAYOR QUE 1":{SPC
}I=2
117{SPC}X=0:{SPC}Y=6:{SPC}GOSUB{SPC}2000
:
118{SPC}PRINT{SPC}TAB(I);" ^"
120{SPC}GOSUB{SPC}3000:{SPC}GOTO{SPC}20
130{SPC}K=VAL(MID$(M$,2))
140{SPC}IF{SPC}K<2{SPC}THEN{SPC}I=-1:{SP
C}GOTO{SPC}110
150{SPC}X=0:{SPC}Y=2:{SPC}GOSUB{SPC}2000
155{SPC}PRINT{SPC}" MODO : ";M1$;"    CL
AVE :";K
160{SPC}X=0:{SPC}Y=4:{SPC}GOSUB{SPC}2000
:{SPC}PRINT{SPC}"  TEXTO:
                "
170{SPC}PRINT:{SPC}INPUT{SPC}T$
171{SPC}FOR{SPC}I=2{SPC}TO{SPC}LEN(T$)
```

```
172{SPC}IF{SPC}I>=LEN(T$){SPC}THEN{SPC}1
74
173{SPC}IF{SPC}MID$(T$,I,1)=" "{SPC}THEN
{SPC}T$=MID$(T$,{SPC4}1,I-1)+MID$(T$,I+1
):{SPC}GOTO{SPC}172
174{SPC}NEXT{SPC}I
175{SPC}IF{SPC}T$="0"{SPC}THEN{SPC}9999
176{SPC}FORQ=1304TO1383:POKEQ,32:NEXTQ
180{SPC}LT=LEN(T$)
190{SPC}IF{SPC}LT>0{SPC}THEN{SPC}220
200{SPC}X=0:Y=4:{SPC}GOSUB{SPC}2000
205{SPC}PRINT{SPC}"?"
210{SPC}GOTO{SPC}170
220{SPC}X=0:{SPC}Y=4:{SPC}GOSUB{SPC}2000
225{SPC}PRINT{SPC}" TEXTO :  ";T$;"
  "
230{SPC}PRINT
240{SPC}S=2*(K-1)
250{SPC}IF{SPC}LEFT$(M$,1)="D"{SPC}THEN(
SPC}390
260{SPC}FOR{SPC}I=1{SPC}TO{SPC}LT{SPC}ST
EP{SPC}S
270{SPC}PRINT{SPC}MID$(T$,I,1);
275{SPC}NEXT{SPC}I
276{SPC}IF{SPC}K=2{SPC}THEN{SPC}350
280{SPC}FOR{SPC}I=1{SPC}TO{SPC}K-2
290{SPC}FOR{SPC}J=1{SPC}TO{SPC}LT{SPC}ST
EP{SPC}S
300{SPC}IF{SPC}J+I<=LT{SPC}THEN{SPC}PRIN
T{SPC}MID$(T$,J+I,1);
310{SPC}IF{SPC}J+S-I<=LT{SPC}THEN{SPC}PR
INT{SPC}MID$(T$,J+S-I,1);
330{SPC}NEXT{SPC}J
340{SPC}NEXT{SPC}I
350{SPC}FOR{SPC}I=K{SPC}TO{SPC}LT{SPC}ST
EP{SPC}S
360{SPC}PRINT{SPC}MID$(T$,I,1);
370{SPC}NEXT{SPC}I
380{SPC}GOTO{SPC}9999
390{SPC}C$=" ":{SPC}FOR{SPC}JJ=1{SPC}TO{
SPC}LT-1:{SPC}C$=C$+" ":{SPC4}NEXT{SPC}J
J
400{SPC}L=0
410{SPC}FOR{SPC}I=1{SPC}TO{SPC}LT{SPC}ST
EP{SPC}S
420{SPC}L=L+1
430{SPC}C$=LEFT$(C$,I-1)+MID$(T$,L,1)+{S
PC10}MID$(C$,I+1)
440{SPC}NEXT{SPC}I
441{SPC}IF{SPC}K=2{SPC}THEN{SPC}560
450{SPC}FOR{SPC}I=1{SPC}TO{SPC}K-2
460{SPC}FOR{SPC}J=1{SPC}TO{SPC}LT{SPC}ST
EP{SPC}S
470{SPC}IF{SPC}J+I>LT{SPC}THEN{SPC}500
480{SPC}L=L+1
490{SPC}C$=LEFT$(C$,I+J-1)+MID$(T$,L,1)+
{SPC8}MID$(C$,I+J+1)
500{SPC}IF{SPC}J+S-I>LT{SPC}THEN{SPC}530
510{SPC}L=L+1
520{SPC}C$=LEFT$(C$,J+S-I-1)+MID$(T$,L,1
)+{SPC6}MID$(C$,J+S-I+1)
530{SPC}NEXT{SPC}J
540{SPC}NEXT{SPC}I
560{SPC}FOR{SPC}I=K{SPC}TO{SPC}LT{SPC}ST
EP{SPC}S
570{SPC}L=L+1
580{SPC}C$=LEFT$(C$,I-1)+MID$(T$,L,1)+{S
PC10}MID$(C$,I+1)
590{SPC}NEXT{SPC}I
600{SPC}PRINT{SPC}C$;"          "
610{SPC}X=2:{SPC}Y=21:{SPC}GOSUB{SPC}200
0
615{SPC}PRINT{SPC}CHR$(18);{SPC25}"DESEA
 CONTINUAR (S/N)"
620{SPC}GET{SPC}R$
640{SPC}IF{SPC}R$="N"{SPC}THEN{SPC}9999
650{SPC}IF{SPC}R$<>"S"{SPC}THEN{SPC}620
680{SPC}K=K+1
690{SPC}X=20:{SPC}Y=2:{SPC}GOSUB{SPC}200
0
695{SPC}PRINT{SPC}K
700{SPC}GOTO{SPC}220
2000{SPC}POKE{SPC}214,Y:{SPC}PRINT:{SPC}
PRINT{SPC}TAB(X);:{SPC7}RETURN
3000{SPC}POKE{SPC}198,0
3010{SPC}X=10:{SPC}Y=21:{SPC}GOSUB{SPC}2
000
3020{SPC}PRINT{SPC}CHR$(18);{SPC}" PULSE
 UNA TECLA "
3030{SPC}GET{SPC}RR$:{SPC}IF{SPC}RR$=""(
SPC}THEN{SPC}3030
3040{SPC}RETURN
9999{SPC}END
```

COLUMNAS COMPLETAS

```
10 REM   **  COLUMNAS COMPLETAS  **
15 POKE 53280,11: POKE53281,11:
   POKE 646,3
20 PRINT CHR$(147)
25 PRINT CHR$(18);"PROGRAMA{SPC}DE{SPC}C
IFRADO{SPC}'COLUMNAS{SPC}COMPLETAS."
30 X=2: Y=2: GOSUB 2000
35 PRINT "MODO{SPC}Y{SPC}CLAVE:": PRINT
40 INPUT M$
50 IF M$="0" THEN 9999
60 IF LEN(M$)<3 THEN I=0: GOTO 80
65 M1$=LEFT$(M$,1)
70 IF M1$="D" OR M1$="C" THEN 100
75 I=1
80 X=0: Y=8: GOSUB 2000: PRINT "ERROR{SP
C}";
82 IF I=1 THEN PRINT "EN{SPC}EL{SPC}MODO
{SPC}(C/D)"
84 IF I=0 THEN PRINT "MENOS{SPC}DE{SPC}3
{SPC}CARACTERES"
```

```
90 GOSUB 3000: GOTO 20
100 K$=MID$(M$,2)
104 X=0: Y=2: GOSUB 2000: PRINT "{SPC}MO
DO{SPC2}:{SPC}";M1$;
105 PRINT "{SPC20}"
106 PRINT : PRINT"{SPC}CLAVE{SPC}:{SPC}"
;K$
107 CC=91: REM ASC("[")
110 LK=LEN(K$)
120 DIM K(LK)
130 FOR I=1 TO LK
140 B=CC
160 FOR J=1 TO LK
170 IF ASC(MID$(K$,J,1)) >= B THEN 200
180 B=ASC(MID$(K$,J,1))
190 P=J
200 NEXT J
210 K$=LEFT$(K$,P-1)+CHR$(91)+MID$(K$,P+
1)
215 K(I)=P
220 NEXT I
230 X=1: Y=6: GOSUB 2000
235 PRINT "TEXTO{SPC}:{SPC}": PRINT
240 INPUT "{SPC}";T$
245 FORQ=1384TO1463:POKEQ,32:NEXTQ
250 FOR I=2 TO LEN(T$)
260 IF I>= LEN(T$) THEN 300
270 IF MID$(T$,I,1)<>"{SPC}" THEN 300
280 T$= LEFT$(T$,I-1)+MID$(T$,I+1)
290 GOTO 260
300 NEXT I
310 IF T$="0" THEN 9999
320 IF LEN(T$)>0 THEN 350
330 X=0: Y=6: GOSUB 2000
335 PRINT "???"
340 GOTO 230
350 LT=LEN(T$)
360 IF LT/LK=INT(LT/LK) THEN 390
370 T$=T$+"Z"
380 GOTO 350
390 X=0: Y=6: GOSUB 2000
395 PRINT "{SPC}TEXTO{SPC}:{SPC8}"
400 X=9: Y=6: GOSUB 2000
405 PRINT T$
406 X=9: Y=10:GOSUB 2000
410 IF M1$="D" THEN 480
420 FOR I=1 TO LK
430 FOR J=K(I) TO LT STEP LK
440 PRINT MID$(T$,J,1);
450 NEXT J
460 NEXT I
470 GOTO 9999
480 DIM C$(LT)
490 L=0
500 FOR I=1 TO LK
510 FOR J=K(I) TO LT STEP LK
520 L=L+1
530 C$(J)=MID$(T$,L,1)
540 NEXT J
550 NEXT I
560 FOR J=1 TO LT
570 PRINT C$(J);
580 NEXT J
590 GOTO 9999
2000 POKE 214,Y: PRINT: PRINT TAB(X);: R
ETURN
3000 POKE 198,0
3010 X=10: Y=21: GOSUB 2000
3020 PRINT CHR$(18); "{SPC}PULSE{SPC}UNA
{SPC}TECLA{SPC}"
3030 GET RR$: IF RR$="" THEN 3030
3040 RETURN
9999 Y=21: GOSUB 2000: END
```

TRANSPOSICION DE ITINERARIO

```
10 REM ** TRASPOSICION DE ITINERARIO **
20 DIM L$(50)
30 FOR R=1 TO 32
40 READ L$(R)
50 NEXT R
60 DATA  "AFKPUBGLQVCHMRWDINSXEJOTY"
70 DATA  "UPKFAVQLGBWRMHCXSNIDYTOJE"
80 DATA  "EJOTYDINSXCHMRWBGLQVAFKPU"
90 DATA  "YTOJEXSNIDWRMHCVQLGBUPKFA"
100 DATA "ABCDEFGHIJKLMNOPQRSTUVWXY"
110 DATA "UVWXYPQRSTKLMNOFGHIJABCDE"
120 DATA "EDCBAJIHGFONMLKTSRQPYXWVU"
130 DATA "YWXVUTSRQPONMLKJIHGFEDCBA"
140 DATA "OSVXYJNRUWFIMQTCEHLPABDGK"
150 DATA "OJFCASNIEBVRMHDXUQLGYWTPK"
160 DATA "ACFJOBEINSDHMRVGLQUXKPTWY"
170 DATA "YXVSOWURNJTQMIFPLHECKGDBA"
180 DATA "KPTWYGLQUXDHMRVBEINSACFJO"
190 DATA "KGDBAPLHECTQMIFWURNJYXVSO"
200 DATA "ABDGKCEHLPFIMQTJNRUWOSVXY"
210 DATA "YWTPKXUQLGVRMHDSNIEBOJFCA"
220 DATA "EFOPYDGNQXCHMRWBILSVAJKTU"
230 DATA "YPOFEXQNGDWRMHCVSLIBUTKJA"
240 DATA "AJKTUBILSVCHMRWDGNQXEFOPY"
250 DATA "UTKJAVSLIBWRMHCXQNGDYPOFE"
260 DATA "ABCDEJIHGFKLMNOTSRQPUVWXY"
270 DATA "UVWXYTSRQPKLMNOJIHGFABCDE"
280 DATA "EDCBAFGHIJONMLKPQRSTYXWVU"
290 DATA "YXWVUPQRSTONMLKFGHIJEDCBA"
300 DATA "ABFGOCEHNPDIMQVJLRUWKSTXY"
310 DATA "YXTSKWURLJVQMIDPNHECOGFBA"
320 DATA "ACDJKBEILSFHMRTGNQUXOPVWY"
330 DATA "YWVPOXUQNGTRMHFSLIEBKJDCA"
340 DATA "OPVWYGNQUXFHMRTBEILSACDJK"
```

```
350 DATA "KJDCASLIEBTRMHFXUQNGYWVPO"
360 DATA "KSTXYJLRUWDIMQVCEHNPABFGO"
370 DATA "OGFBAPNHECVQMIDWURLJYXTSK"
375 DEF FN A(X)=1477+X+40*Y
376 DEF FN B(X)=PEEK(1477+X+40*Y)
377 CA=64
380 PRINT CHR$(147);CHR$(18);
390 PRINT "{SPC}CIFRADO{SPC}POR{SPC}TRAS
POSICION{SPC}DE{SPC}ITINERARIO{SPC}"
400 POKE214,2:PRINT:PRINT TAB(2);
    "MODO{SPC}(NUMERO{SPC}CLAVE){SPC}";
410 INPUT M$
420 IF M$="0" THEN 9999
430 IF M$="L" THEN 1010
440 IF M$="S" THEN 1510
450 LM=LEN(M$)
460 IF LM<2 THEN 520
470 IF MID$(M$,1,1)<"C" OR
      MID$(M$,1,1)>"D" THEN 520
480 FOR I=2 TO LM
490 IF MID$(M$,I,1)<"0" OR
      MID$(M$,I,1)>"9" THEN 520
500 NEXT I
510 GOTO 540
520 POKE214,2:PRINT:PRINT "?"
530 GOTO 400
540 K=VAL(MID$(M$,2))
550 IF K<1 OR K>=R THEN 520
560 POKE214,2:PRINT:PRINT "MODO{SPC}:{SP
C}";        LEFT$(M$,1);"{SPC3}NUMERO{SP
C}CLAVE{SPC}:";K
561 POKE214,4:PRINT:PRINT "RUTA{SPC}:{SP
C15}"
562 FOR Y=0 TO 4
563 POKE214,5+Y:PRINT:PRINT TAB(9);
    MID$(L$(K),Y*5+1,5)
564 NEXT Y
565 POKE 214,4: PRINT: PRINT TAB(8);
    CHR$(111);
566 FOR Y=1 TO 5 : PRINT CHR$(183);:
    NEXT: PRINTCHR$(112)
567 FOR Y=1 TO 5 : PRINT TAB(8);
    CHR$(165);TAB(14);CHR$(167):NEXT
568 PRINTTAB(8);CHR$(108);
569 FOR Y=1 TO 5 : PRINT CHR$(175);:
    NEXT: PRINTCHR$(186)
570 POKE 214,12:PRINT:PRINT;"TEXTO:";
580 INPUT T$
585 I1=LEN(T$)
590 FOR I=1 TO LEN(T$)
600 IF I>LEN(T$) THEN 670
610 IF MID$(T$,I,1)<>"{SPC}" THEN 670
620 R$=""
630 IF I>1 THEN R$=MID$(T$,1,I-1)
640 IF I<LEN(T$) THEN R$=R$+MID$(T$,I+1)
650 T$=R$
660 GOTO 600
670 NEXT I
680 IF T$="0" THEN 9999
690 LT=LEN(T$)
700 IF LT>0 THEN 730
710 POKE 214,12: PRINT: PRINT"?"
720 GOTO580
730 IF LT/25=INT(LT/25) THEN 770
740 T$=T$+"Z"
750 LT=LT+1
760 GOTO 730
770 POKE 214,12: PRINT: PRINT"TEXTO{SPC}
:{SPC}";     T$;
775 IF I1>LT THEN FOR I=LT TO I1+2:
    PRINT "{SPC}";:NEXT
780 PRINT: PRINT
790 IF LEFT$(M$,1)="D" THEN 910
800 C$=""
810 FOR J=1 TO 25
820 FOR I=1 TO 25
830 IF MID$(L$(K),J,1)<>CHR$(CA+I)
    THEN 840
835 C$= LEFT$(C$,J-1) + MID$(T$,I,1) +
    MID$(C$,J+1)
840 NEXT I
850 NEXT J
860 PRINT C$;
870 IF LT=25 THEN 9999
880 T$=MID$(T$,26)
890 LT=LT-25
900 GOTO 800
910 C$=""
920 FOR I=1 TO 25
930 FOR J=1 TO 25
940 IF MID$(L$(K),J,1)<>CHR$(CA+I)
    THEN 950
945 C$= LEFT$(C$,I-1) + MID$(T$,J,1) +
    MID$(C$,I+1)
950 NEXT J
960 NEXT I
970 PRINT C$;
975 IF LT=25 THEN 9999
980 T$=MID$(T$,26)
990 LT=LT-25
1000 GOTO 910
1010 IF R<=50 THEN 1070
1020 POKE 214,2: PRINT: PRINT "?"
1030 POKE 214,4: PRINT:
     PRINT"ARCHIVOS{SPC}COMPLETOS"
1050 POKE 214,2: PRINT: PRINT TAB(22);
1060 GOTO 410
1070 POKE 214,2: PRINT:
     PRINT "NUMERO{SPC}DE{SPC}RUTA{SPC}:
";
1075 PRINT  STR$(R);"{SPC7}"
1080 POKE 214,9: PRINT: PRINT TAB(12);
     CHR$(111);
1090 FOR Y=1 TO 5 : PRINT CHR$(183);:
     NEXT: PRINT CHR$(112)
1100 FOR Y=1 TO 5 : PRINT TAB(12);
     CHR$(165);TAB(18);CHR$(167):NEXT
1110 PRINT TAB(12);CHR$(108);
1120 FOR Y=1 TO 5 : PRINT CHR$(175);:
     NEXT: PRINTCHR$(186)
1130 X=0
1140 Y=0
1150 I=FN B(X):IF I<>160 THEN
     I1=I: I=-31
1155 IF I<-30 THEN I=1:POKE FN A(X),I1
1157 IF I>30 THEN I=-1:POKE FN A(X),160
1160 GET R$
1170 IF R$="" THEN I=2*I: GOTO 1155
1185 IF R$="0" THEN 9999
1190 IF R$=CHR$(13) THEN 1320
1200 IF R$=CHR$(29) AND X+Y<8 THEN 1290
1210 IF R$<>CHR$(157) OR X+Y=0 THEN 1250
```

```
1220 GOSUB 1600: X=X-1
1230 IF X<0 THEN X=4: Y=Y-1
1240 GOTO 1150
1250 IF R$=CHR$(17) AND Y<4 THEN
     GOSUB 1600: Y=Y+1: GOTO 1150
1260 IF R$=CHR$(145) AND Y>0 THEN
     GOSUB 1600: Y=Y-1: GOTO 1150
1270 IF (R$<"A" OR R$>"Y") AND
     R$<>"{SPC}" THEN 1150
1280 IF R$<>"{SPC}" THEN I1=ASC(R$)-CA
1290 GOSUB 1600
1295 IF X+Y<8 THEN X=X+1
1300 IF X>4 THEN Y=Y+1: X=0
1310 GOTO 1150
1320 GOSUB 1600: C$=""
1330 FOR Y=0 TO 4
1340 FOR X=0 TO 4
1350 R$=CHR$(FN B(X)+CA)
1360 IF R$<>CHR$(96) THEN 1400
1370 POKE FN A(X),23
1390 GOTO 1130
1400 C=ASC(R$)-CA
1410 IF MID$(C$,C,1)=R$ THEN 1370
1420 C$=LEFT$(C$,C-1)+R$+MID$(C$,C+1)
1430 NEXT X
1440 NEXT Y
1450 FOR Y=0 TO 4
1460 FOR X=0 TO 4
1470 I=FN B(X)+CA: IF I=96 THEN I=32
1475 L$(R)=L$(R)+CHR$(I)
1480 NEXT X
1490 NEXT Y
1495 R=R+1
1500 GOTO 1700
1510 POKE 214,6: PRINT: PRINT TAB(2);
     "NOMBRE{SPC}";
1520 INPUT R$
1524 IF R$="0" THEN 9999
1525 IF LEN(R$)>14 THEN R$=LEFT$(R$,14)
1526 POKE 214,6: PRINT: PRINT "{SPC}NOMB
RE{SPC}:{SPC2}";R$; "{SPC20}"
1530 SAVE R$
1540 GOTO 380
1600 POKE FN A(X),I1: RETURN
1700 PRINT CHR$(147): PRINT: PRINT
1710 PRINT 10000+(R-1)*10; "DATA{SPC}";
          CHR$(34);L$(R-1); CHR$(34)
1720 PRINT "30{SPC}FOR{SPC}R=1{SPC}TO";R
-1
1730 PRINT "RUN"
1740 POKE 198,8
1750 FOR I=631 TO 634: POKE I,13: NEXT
1760 PRINT CHR$(19)
1770 POKE 198,3
1780 END
1790 REM ATENCION NO QUITE LA SENTENCIA
     ANTERIOR "END"
9999 POKE 214,21: PRINT
```

REJILLA DE CARDANO

```
10 REM   ** REJILLA DE CARDANO **
15 GOSUB 2200
20 PRINT CHR$(147);CHR$(18);
25 PRINT "{SPC4}CIFRADO{SPC}DE{SPC}LA{SP
C}REJILLA{SPC}DE{SPC}CARDANO{SPC4}"
30 POKE 214,2: PRINT: PRINT TAB(2);
   "MODO{SPC}";
40 INPUT M$
50 IF M$="0" THEN 9999
60 IF M$="C" OR M$="D" THEN 90
70 POKE 214,2: PRINT: PRINT "?"
80 GOTO 30
90 POKE 214,2: PRINT: PRINT "{SPC}MODO{S
PC}:{SPC}";     M$; "{SPC14}"
95 DIM G(6,6)
97 NH=0
100 POKE 214,11: PRINT:
    PRINT TAB(23); CHR$(176);
110 FOR I=1 TO 7: PRINT CHR$(192);:
    NEXT: PRINT CHR$(174)
120 FOR I=1 TO 7: PRINT TAB(23);
    CHR$(194);TAB(27);CHR$(194);
130 PRINT TAB(31);CHR$(194): NEXT
140 PRINT TAB(23);CHR$(173);
150 FOR I=1 TO 7: PRINT CHR$(192);:
    NEXT: PRINT CHR$(189)
160 POKE 214,15: PRINT:
    PRINT TAB(23); CHR$(171);
170 FOR I=1 TO 7: PRINT CHR$(192);:
    NEXT: PRINT CHR$(179)
180 POKE 214,11: PRINT:
    PRINT TAB(27); CHR$(178);
181 POKE 214,15: PRINT:
    PRINT TAB(27); CHR$(219);
182 POKE 214,19: PRINT:
    PRINT TAB(27); CHR$(177);
190 FOR Q=1 TO 4
200 SX=24
210 IF Q=2 OR Q=3 THEN SX=28
220 SY=12
230 IF Q>2 THEN SY=16
240 POKE 214,SY: PRINT: PRINT TAB(SX);
    "123"
250 PRINT TAB(SX);"456":
    PRINT TAB(SX);"789"
255 POKE 214,4: PRINT: PRINT "CUADRO";
    Q;"AGUJERO:"
260 POKE 214,4: PRINT: PRINT TAB(18);
    "{SPC}"; CHR$(157);
270 GET R$
280 IF R$="" THEN 270
290 IF R$="0" THEN 9999
300 IF R$="N" THEN 620
310 IF R$>="1" AND R$<="9" THEN 350
320 POKE 214,4: PRINT: PRINT TAB(18);
    "?"
```

```
330 GOSUB 2300
340 GOTO 260
350 V=VAL(R$)
360 PRINT CHR$(157);V
370 GY=INT((V-1)/3)+1
380 GX=V-3*(GY-1)
390 IF Q=2 OR Q=3 THEN GX=GX+3
400 IF Q>2 THEN GY=GY+3
410 IF G(GY,GX)=1 THEN 330
420 FOR Y=1 TO 6
430 FOR X=1 TO 6
440 IF G(Y,X)=0 THEN 530
450 YY=Y
460 XX=X
470 FOR R=1 TO Q-1
480 I=YY
490 YY=XX
500 XX=7-I
510 IF YY=GY AND XX=GX THEN 330
520 NEXT R
530 NEXT X
540 NEXT Y
550 G(GY,GX)=1
560 IF GX>3 THEN GX=GX+1
570 IF GY>3 THEN GY=GY+1
580 POKE 214,11+GY: PRINT:
    PRINT TAB(23+GX);CHR$(18);"{SPC}"
590 NH=NH+1
600 IF NH<9 THEN 260
610 Q=4
620 IF Q=4 AND NH<9 THEN 320
630 FOR I=0 TO 2
640 FOR J=0 TO 2
650 IF   PEEK (1064+(SY+I)*40+SX+J)<>160
    THEN POKE (1064+(SY+I)*40+SX+J),32
660 NEXT J
670 NEXT I
680 NEXT Q
690 POKE 214,4: PRINT: PRINTTAB(18);"{SP
C3}"
700 POKE 214,6: PRINT:
    PRINT TAB(2);"TEXTO{SPC}";
710 INPUT T$
720 R$="": T$=T$+"{SPC}"
730 FOR I=1 TO LEN(T$)
740 IF MID$(T$,I,1)<>"{SPC}" THEN
        R$=R$+MID$(T$,I,1)
800 NEXT I
805 T$=R$
810 IF T$="0" THEN 9999
820 LT=LEN(T$)
830 IF LT/36=INT(LT/36) THEN 870
840 T$=T$+"Z"
850 LT=LT+1
860 GOTO830
870 POKE 214,6: PRINT:
    PRINT "{SPC}TEXTO{SPC}:{SPC}";T$;"{S
PC10}"
880 PRINT
890 DIM C$(6,6)
895 RF=1
900 IF M$="D" THEN 1110
910 CN=0
920 FOR Q=1 TO 4
930 FOR Y=1 TO 6
940 FOR X=1 TO 6
950 IF G(Y,X)=0 THEN 980
960 CN=CN+1
970 C$(Y,X)=MID$(T$,CN,1)
980 NEXT X
990 NEXT Y
1000 GOSUB 2000
1010 NEXT Q
1020 FOR Y=1 TO 6
1030 FOR X=1 TO 6
1040 PRINT C$(Y,X);
1050 NEXT X
1060 NEXT Y
1070 IF LT<37 THEN 9999
1080 T$=MID$(T$,37)
1090 LT=LT-36
1100 GOTO 910
1110 CN=0
1120 FOR Y=1 TO 6
1130 FOR X=1 TO 6
1140 CN=CN+1
1150 C$(Y,X)=MID$(T$,CN,1)
1160 NEXT X
1170 NEXT Y
1180 FOR Q=1 TO 4
1190 FOR Y=1 TO 6
1200 FOR X=1 TO 6
1210 IF G(Y,X)>0 THEN PRINT C$(Y,X);
1220 NEXT X
1230 NEXT Y
1240 GOSUB 2000
1250 NEXT Q
1260 IF LT<37 THEN 9999
1270 T$=MID$(T$,37)
1280 LT=LT-36
1290 GOTO 1110
2000 FOR Y=1 TO 6
2010 FOR X=1 TO 6
2020 IF G(Y,X)<>RF THEN 2070
2030 G(Y,X)=0
2040 YY=X
2050 XX=7-Y
2060 G(YY,XX)=3-RF
2070 NEXT X
2080 NEXT Y
2090 RF=3-RF
2100 RETURN
2200 POKE 53280,0: POKE 53281,7:
2210 POKE 646,0: PRINTCHR$(147)
2220 FOR I=54272 TO 54295: POKE I,0:NEXT
2230 POKE 54272,200: POKE54273,100
2240 POKE 54277,0  : POKE54278,128
2250 POKE 54276,32 : POKE54296,15
2260 RETURN
2300 POKE 54276,33
2310 FOR S9=0 TO 500:NEXT
2320 POKE 54276,32
2330 RETURN
9999 POKE 214,21: PRINT
```

ANALISIS POR COLUMNAS COMPLETAS

```
10 REM ANALISIS POR COLUMNAS COMPLETAS
15 GOSUB 8300
16 DIM C$(20,15),P$(20,15)
17 DIM B(15),F(15),C(20),R(20)
20 PRINT: PRINT "{SPC}POSICIONE{SPC}SU{S
PC}CASSETE{SPC}CON{SPC}EL{SPC}FICHERO{SP
C}DE{SPC2}DATOS."
25 FOR I=1 TO 20: FOR J=1 TO 15:
   C$(I,J)="{SPC}":P$(I,J)="{SPC}": NEXT
 J,I
26 PRINT "{SPC}DESPUES{SPC}PULSE{SPC}CUA
LQUIER{SPC}TECLA."
30 GOSUB 8400: POKE 198,0
40 GET R$: IF R$="" THEN 40
50 GOSUB 5000 : REM LEE FRECUENCIAS
60 GOSUB 6000 : REM LEE TRANSICIONES
70 PRINT CHR$(147); CHR$(18);
80 PRINT "{SPC4}ANALISIS{SPC}POR{SPC}COL
UMNAS{SPC}COMPLETAS.{SPC4}";
85 PRINT "{SPC40}"
90 POKE 214,2: PRINT:
   PRINT "{SPC2}TEXTO{SPC}";
100 INPUT T$
110 R$="": T$=T$+"{SPC}"
120 FOR I=1 TO LEN(T$)
130 IF MID$(T$,I,1)<>"{SPC}" THEN
       R$=R$+MID$(T$,I,1)
140 NEXT I
150 T$=R$
200 IF T$="0" THEN 9999
210 LT=LEN(T$)
220 IF LT>0 THEN 250
230 POKE 214,2: PRINT: PRINT "?"
240 GOSUB 8400: GOTO 90
250 NF=0
260 FOR I=2 TO INT(LT/2)
270 IF LT/I=INT(LT/I) THEN NF=NF+1
280 NEXT I
290 IF NF=0 THEN 230
300 FOR V9=1 TO NF: C(V9)=0: R(V9)=0:
310 NEXT V9
320 NF=0
330 FOR I=2 TO INT(LT/2)
340 IF LT/I>INT(LT/I) THEN 380
350 NF=NF+1
360 C(NF)=I
370 R(NF)=LT/I
380 NEXT I
390 CA=64
400 POKE 214,2: PRINT: PRINT "TEXTO{SPC}
:";     T$;"{SPC29}"
405 PRINT
410 PRINT "{SPC}HAY";NF;
       "FORMAS{SPC}DE{SPC}FACTORIZAR"
420 PRINT
430 FOR I=1 TO NF
440 PRINT CHR$(18);CHR$(28);:
    S8=I: GOSUB 8500: PRINT "{SPC4}";
441 PRINT CHR$(31);"{SPC3}";:S8=C(I):
      GOSUB 8500:      PRINT "{SPC}COLUM
NAS,{SPC}";
442 PRINT MID$(STR$(R(I)),2);"{SPC}FILAS
."
445 NEXT I
450 PRINT
460 PRINT "{SPC2}PULSE{SPC}CUALQUIER{SPC
}TECLA{SPC}PARA{SPC}EL{SPC}CALCULO{SPC2}
DE{SPC}VOCALES.";
470 PRINT "{SPC}ESPACIO{SPC}PARA{SPC}CON
TINUAR."
475 GOSUB 8400
480 GET R$
490 IF R$="" THEN 480
500 IF R$="0" THEN 9999
505 IF R$="C" THEN PRINT "CONSULTE{SPC}E
L{SPC}APENDICE": GOTO 450
510 IF R$="{SPC}" THEN 650
515 PRINT CHR$(147)
520 FOR I=1 TO NF
530 PRINT CHR$(18);CHR$(28);
    MID$(STR$(I),2);"{SPC2}";
531 PRINT CHR$(31);TAB(6);STR$(C(I));
    "{SPC}X";STR$(R(I));"{SPC}:{SPC}";CH
R$(146);
540 FOR J=1 TO R(I)
550 NV=0
560 FOR K=1 TO C(I)
570 R$=MID$(T$,(K-1)*R(I)+J,1)
580 IF R$="A" OR R$="E" OR R$="I" OR R$=
    "O" OR R$="U" THEN NV=NV+1
590 NEXT K
600 PRINT INT(NV/C(I)*100);CHR$(157);"%"
    ;
610 NEXT J
620 PRINT
630 PRINT
640 NEXT I
650 PRINT
660 PRINT "{SPC2}INTRODUZCA{SPC}EL{SPC}N
UMERO{SPC}DE{SPC}LA{SPC}OPCION{SPC}SE-{S
PC}LECCIONADA";: INPUT R$
663 IF R$="C" THEN PRINT "CONSULTE{SPC}E
L{SPC}APENDICE": GOTO 660
665 BD=VAL(R$)
667 IF BD=0 THEN 9999
670 IF BD<1 OR BD>NF OR BD>INT(BD)
    THEN 660
680 NC=C(BD)
690 NR=R(BD)
691 FOR V9=1 TO NR: FOR V8=1 TO NC:
    C$(V9,V8)="{SPC}": NEXT V8,V9
692 FOR I=1 TO NR
693 FOR J=1 TO NC
694 C$(I,J)=MID$(T$,(J-1)*NR+I,1)
695 NEXT J
696 NEXT I
```

```
697 FOR V9=1 TO NC: B(V9)=0: F(V9)=0:
698 NEXT V9
700 PRINT CHR$(147)
710 FOR I=1 TO NC
720 PRINT CHR$(19);TAB(I-1);:
    S8=INT(I/10): GOSUB 8500:
725 PRINT TAB(15+I);:S8=INT(I/10):
    GOSUB 8500: PRINT
730 PRINT TAB(I-1);:S8=I-10*INT(I/10):
    GOSUB 8500
735 PRINT TAB(15+I);:S8=INT(I/10):
    GOSUB 8500: PRINT
740 PRINT TAB(I-1);CHR$(192);
745 PRINT TAB(15+I);CHR$(192)
750 NEXT I
760 FOR I=1 TO NR
765 FOR J=1 TO NC
770 PRINT C$(I,J);
775 NEXT J
780 PRINT
790 NEXT I
800 GOSUB 8002
810 F(CN)=1
820 B(1)=CN
830 GOSUB 8100
840 POKE 214,21: PRINT: PRINT "{SPC39}"
845 POKE 214,21: PRINT: PRINT "{SPC5}PUL
SE{SPC}B,C,D,I,L,N,P,R,S,W,0"
850 GET R$
860 IF R$="" THEN 850
865 POKE 214,21: PRINT: PRINT "{SPC39}"
867 IF R$="N" THEN 697
870 IF R$="B" THEN PRINT CHR$(147):
    GOTO 450
880 IF R$="C" THEN POKE211,5:POKE214,16:
SYS58640:PRINT"CONSULTE{SPC}EL{SPC}APEND
ICE": GOTO 840
890 IF R$="0" THEN 9999
900 IF R$<>"L" AND R$<>"R" THEN 1160
910 GOSUB 8050
915 IF B(PC)=0 THEN 910
920 C=B(PC)
930 GOSUB 8220
970 POKE 214,SY: PRINT:
980 FC=32
990 IF 22-SY>INT(NC/2) THEN FC=6
1000 IF 22-SY>NC-1 THEN FC=13
1010 FOR I=1 TO NC
1020 IF I=C THEN 1140
1030 IF F(I)=0 THEN PRINT CHR$(18);I;
1040 IF F(I)>0 THEN PRINT I;
1050 PRINT "{SPC}";
1060 P=0
1070 FOR J=1 TO NR
1080 CP=ASC(C$(J,C))-CA
1090 TC=ASC(C$(J,I))-CA
1100 IF R$="L" THEN P=P+T(TC,CP)
1110 IF R$="R" THEN P=P+T(CP,TC)
1120 NEXT J
1130 PRINT P;CHR$(FC);
1140 NEXT I
1150 REM ________________________________
1151 PRINTCHR$(17);"PULSE{SPC}";CHR$(18)
;"RETURN";":{SPC}";:INPUT R$
1152 GOSUB 8220
1153 GOTO 840
1160 IF R$<>"D" THEN 1250
1170 GOSUB 8050
1175 IF B(PC)>0 THEN F(B(PC))=0
1180 FOR I=PC TO NC-1
1190 B(I)=B(I+1)
1200 IF B(I)>0 THEN F(B(I))=I
1210 NEXT I
1220 B(I)=0
1230 GOSUB 8100
1240 GOTO 840
1250 IF R$<>"I" THEN 1301
1255 GOSUB 8050
1257 IF B(NC)>0 THEN F(B(NC))=0
1260 FOR I=NC TO PC+1 STEP -1
1270 B(I)=B(I-1)
1280 IF B(I)>0 THEN F(B(I))=I
1290 NEXT I
1300 GOTO 1220
1301 IF R$<>"W" THEN 1310
1302 GOSUB 8050
1303 GOSUB 8002
1304 IF B(PC)>0 THEN F(B(PC))=0
1305 F(CN)=PC
1306 B(PC)=CN
1307 GOSUB 8100
1308 GOTO 840
1310 IF R$<>"P" THEN 1319
1311 INPUT "{SPC9}LETRAS{SPC7}";R$
1312 IF LEN(R$)<>2 THEN 1311
1313 L1=ASC(LEFT$(R$,1))-CA
1314 L2=ASC(RIGHT$(R$,1))-CA
1315 IF L1<1 OR L1>26 OR L2<1 OR L2>26
     THEN 1311
1316 GOSUB 8220
1317 POKE 211,30:POKE214,5:SYS58640:PRIN
T R$;":{SPC}";T(L1,L2)
1318 GOTO 840
1319 IF R$="S" THEN 1350
1320 POKE 214,21: PRINT: PRINT "?"
1330 GOSUB 8400
1340 GOTO 840
1350 PRINT CHR$(147)
1360 FOR I=1 TO NR
1365 FOR J=1 TO NC
1370 PRINTP$(I,J);
1375 NEXTJ
1380 NEXT I
1390 GOTO 9999
5000 DIM E(26)
5010 OPEN 1,1,0,"FRECUENCIAS"
5020 FOR I=1 TO 26
5030 INPUT#1,E(I)
5040 NEXT I
5050 CLOSE 1
5060 RETURN
6000 DIM T(26,26)
6010 OPEN 1,1,0,"TRANSICIONES"
6020 FOR I=1 TO 26
6030 FOR J=1 TO 26
6040 INPUT#1,T(I,J)
6050 NEXT J
6060 NEXT I
6070 CLOSE 1
6080 RETURN
8002 POKE211,5:POKE214,20:SYS58640: PRIN
T "QUE{SPC}COLUMNA{SPC}QUIERE{SPC}PONER{
```

```
SPC)";
8005 INPUT CN
8010 CN=INT(CN)
8020 IF CN=0 THEN 9999
8030 IF CN<1 OR CN>NC THEN 8002
8035 IF F(CN)>0 THEN 8002
8040 RETURN
8050 POKE211,0:POKE214,21:SYS58640:INPUT
 "{SPC5}EN{SPC}LA{SPC}POSICION{SPC}";PC:
PRINT"{SPC12}";
8060 PC=INT(PC)
8070 IF PC=0 THEN 9999
8080 IF PC<1 OR PC>NC THEN 8050
8090 RETURN
8100 FOR V9=1 TO NR: FOR V8=1 TO NC:
     P$(V9,V8)="{SPC}": NEXT V8,V9
8110 FOR I=1 TO NC
8115 POKE 214,1: PRINT: PRINT
     TAB(I-1);CHR$(192)
8120 C=F(I)
8130 IF C=0 THEN 8170
8135 POKE 214,1: PRINT: PRINT
     TAB(I-1);CHR$(18);CHR$(192)
8140 FOR J=1 TO NR
8150 P$(J,C)=C$(J,I)
8160 NEXT J
8170 NEXT I
8180 FOR I=1 TO NR
8190 POKE 214,1+I: PRINT: PRINT TAB(16);
8195 FOR S9=1 TO NC: PRINT P$(I,S9);:
     NEXT
8200 NEXT I
8210 RETURN
8220 SY=NR+2
8230 FOR I=SY TO 23
8240 POKE 214,I: PRINT: PRINT "{SPC39}";
8250 NEXT I
8260 RETURN
8300 POKE 53280,0: POKE 53281,7:
8310 POKE 646,0: PRINTCHR$(147)
8320 FOR I=54272 TO 54295: POKE I,0:NEXT
8330 POKE 54272,200: POKE54273,100
8340 POKE 54277,0  : POKE54278,128
8350 POKE 54276,32 : POKE54296,15
8360 RETURN
8400 POKE 54276,33
8410 FOR S9=0 TO 500:NEXT
8420 POKE 54276,32
8430 RETURN
8500 SS$=STR$(S8): PRINT MID$(SS$,2);: R
ETURN
9999 END
```

ANALISIS POR LA REJILLA DE CARDANO

```
10 REM ANALISIS POR 'LA REJILLA DE
              CARDANO'
15 GOSUB 8300
20 PRINT: PRINT "{SPC}POSICIONE{SPC}SU{S
PC}CASSETE{SPC}CON{SPC}EL{SPC}FICHERO{SP
C}DE{SPC2}DATOS."
26 PRINT"{SPC}DESPUES{SPC}PULSE{SPC}CUAL
QUIER{SPC}TECLA."
30 GOSUB 8400: POKE 198,0
40 GET R$: IF R$="" THEN 40
50 GOSUB 5000 : REM LEE FRECUENCIAS
60 GOSUB 6000 : REM LEE TRANSICIONES
65 DIM A(6,6),G(6,6)
70 PRINT CHR$(147); CHR$(18);
80 PRINT "PROGRAMA{SPC}DE{SPC}ANALISIS:{
SPC}REJILLA{SPC}DE{SPC}CARDANO";
85 PRINT "{SPC40}"
90 POKE 214,2: PRINT:
   PRINT "{SPC2}TEXTO{SPC}";
100 INPUT T$
110 R$="": T$=T$+"{SPC}"
120 FOR I=1 TO LEN(T$)
130 IF MID$(T$,I,1)<>"{SPC}" THEN
       R$=R$+MID$(T$,I,1)
140 NEXT I
150 T$=R$
200 IF T$="0" THEN 9999
210 LT=LEN(T$)
220 IF LT=0 THEN 240
230 IF LT/36=INT(LT/36) THEN 260
235 T$=T$+"Z"
240 LT=LT+1
250 GOTO 230
260 POKE 214,2: PRINT: PRINT "TEXTO{SPC}
:{SPC}";     T$;"{SPC8}"
270 NB=INT(LT/36)
310 CA=64
370 POKE 214,21: PRINT: PRINT"{SPC3}PULS
E{SPC}CUALQUIER{SPC}TECLA": POKE198,0
380 GET R$
390 IF R$="" THEN 380
395 IF R$="0" THEN 9999
400 REM INTRODUZCA AQUI LA RUTINA DE
    IMPRESION SI LO DESEA
430 PRINT CHR$(147)
440 FOR I=1 TO 6: FOR J=1 TO 6
450 A(I,J)=0: G(I,J)=0:
460 NEXT J,I
510 PRINT CHR$(19);TAB(13);"123456"
520 FOR I=1 TO 6
530 POKE 214,I+1: PRINT: PRINT TAB(9);I
540 NEXT I
541 NH=0
545 R$=""
550 GOTO 700
560 POKE 214,21: PRINT:
```

```
    PRINT "{SPC}PULSE{SPC}C,D,H,L,R,P,T,
N,0"
570 GET R$
580 IF R$="" THEN 570
585 FOR I=10 TO 20
586 POKE 214,I:PRINT:PRINT"{SPC38}"
587 NEXT I
590 POKE 214,21: PRINT:
    PRINT "{SPC24}"
630 IF R$<>"D" THEN 690
640 GOSUB 8000
650 G(Y,X)=0
660 POKE 214,Y+1: PRINT: PRINT
    TAB(X+12);"{SPC}"
670 NH=NH-1
680 GOTO 560
690 IF R$<>"H" THEN 740
700 GOSUB 8000
710 G(Y,X)=1
720 POKE 214,Y+1: PRINT: PRINT
    TAB(X+12);CHR$(18)+"{SPC}"
725 NH=NH+1
730 GOTO 560
740 IF R$<>"L" AND R$<>"R" THEN 1105
745 GOSUB 8200
750 GOSUB 8000
753 XX=X
757 YY=Y
760 IF R$="L" THEN 830
770 X=X+1
780 IF X<=6 THEN 915
790 X=1
800 Y=Y+1
810 IF Y>6 THEN 560
820 GOTO 880
830 X=X-1
840 IF X>=1 THEN 915
850 X=6
860 Y=Y-1
870 IF Y<1 THEN 560
915 P=0
917 FOR I=1 TO NB
920 FOR J=1 TO 2
960 IF R$<>"R" THEN 970
961 V8=(I-1)*36+(YY-1)*6+XX
962 V9=(I-1)*36+(Y-1)*6+X
963 V8=ASC(MID$(T$,V8,1))-CA
964 V9=ASC(MID$(T$,V9,1))-CA
965 P=P+T(V8,V9)
970 X=7-X
980 Y=7-Y
990 XX=7-XX
1000 YY=7-YY
1010 R$=CHR$(ASC("R")+ASC("L")-ASC(R$))
1020 NEXT J
1025 NEXT I
1030 IN=1
1040 FOR I=1 TO 4
1050 GOSUB 8100
1060 IF G(X,Y)=1 THEN IN=0
1070 NEXT I
1080 IF IN=1 THEN PRINT CHR$(18);
1085 PRINT X;",";Y;CHR$(146);":{SPC2}";P
,
1090 REM
1100 GOTO 560
1105 IF R$="N" THEN 430
1110 IF R$<>"P" THEN 1200
1120 GOSUB 8200
1130 INPUT "LETRAS{SPC}";L$
1140 IF LEN(L$)<>2 THEN 1130
1150 L1=ASC(LEFT$(L$,1))-CA
1160 L2=ASC(RIGHT$(L$,1))-CA
1170 IF L1<1 OR L1>26 OR L2<1 OR L2>26
     THEN 1130
1180 PRINT CHR$(18);L$;CHR$(146);
     ":{SPC2}";T(L1,L2)
1190 GOTO 560
1200 IF R$<>"T" THEN 1460
1205 IF NH=9 THEN 1210
1207 GOSUB 8400
1208 GOTO 560
1210 RF=1
1211 FOR Y=1 TO 6
1212 FOR X=1 TO 6
1213 A(Y,X)=G(Y,X)
1214 NEXT X
1215 NEXT Y
1219 FOR I=1 TO 4
1220 GOSUB 8200
1225 FOR J=1 TO NB
1230 FOR K=1 TO 4
1240 FOR Y=1 TO 6
1250 FOR X=1 TO 6
1260 IF A(Y,X)<>RF THEN 1270
1261 V8=(J-1)*36+(Y-1)*6+X
1262 PRINT MID$(T$,V8,1);
1263 A(Y,X)=0
1264 A(X,7-Y)=3-RF
1270 NEXT X
1280 NEXT Y
1290 RF=3-RF
1300 NEXT K
1310 NEXT J
1320 POKE 214,21: PRINT: PRINT "PULSE{SP
C}C,N,R,S,0{SPC}"
1330 GET R$
1340 IF R$="" THEN 1330
1350 POKE 214,21: PRINT: PRINT "{SPC16}"
1360 IF R$<>"C" THEN 1380
1370 REM CREAR RUTINA DE IMPRESION
1375 GOTO 1320
1380 IF R$<>"N" THEN 1410
1381 FOR Y=1 TO 6
1382 FOR X=1 TO 6
1383 IF A(Y,X)<>RF THEN 1386
1384 A(Y,X)=0
1385 A(X,7-Y)=3-RF
1386 NEXT X
1387 NEXT Y
1388 RF=3-RF
1390 NEXT I
1400 GOTO 1219
1410 IF R$="R" THEN 560
1420 IF R$="S" OR R$="0" THEN 9999
1430 POKE 214,21: PRINT: PRINT "?"
1440 GOSUB 8400
1450 GOTO 1320
1460 IF R$="0" THEN 9999
1470 POKE 214,21: PRINT: PRINT "?"
1480 GOSUB 8400
1490 GOTO 560
```

```
5000 DIM E(26)
5010 OPEN 1,1,0,"FRECUENCIAS"
5020 FOR I=1 TO 26
5030 INPUT#1,E(I)
5040 NEXT I
5050 CLOSE 1
5060 RETURN
6000 DIM T(26,26)
6010 OPEN 1,1,0,"TRANSICIONES"
6020 FOR I=1 TO 26
6030 FOR J=1 TO 26
6040 INPUT#1,T(I,J)
6050 NEXT J
6060 NEXT I
6070 CLOSE 1
6080 RETURN
8000 POKE 214,17:PRINT:
8002 INPUT "POSICION{SPC}X,Y{SPC}";X,Y
8005 IF X=0 OR Y=0 THEN 9999
8010 IF X<1 OR X>6 OR X>INT(X)
     OR Y<1 OR Y>6 OR Y>INT(Y) THEN 8000
8020 IF R$="D" OR R$="L" OR R$="R"
     THEN 8080
8030 FOR I=1 TO 4
8040 GOSUB 8100
8050 IF G(Y,X)<>0 THEN 8090
8060 NEXT I
8070 RETURN
8080 IF G(Y,X)=1 THEN 8070
8090 GOSUB 8400
8095 GOTO 8000
8100 S=Y
8110 Y=7-X
8120 X=S
8130 RETURN
8200 FOR I=10 TO 20
8210 POKE 214,I: PRINT: PRINT "{SPC38}"
8220 NEXT I
8230 POKE 214,10: PRINT
8240 RETURN
8300 POKE 53280,0: POKE 53281,7:
8310 POKE 646,0: PRINTCHR$(147)
8320 FOR I=54272 TO 54295: POKE I,0:NEXT
8330 POKE 54272,200: POKE54273,100
8340 POKE 54277,0  : POKE54278,128
8350 POKE 54276,32 : POKE54296,15
8360 RETURN
8400 POKE 54276,33
8410 FOR S9=0 TO 500:NEXT
8420 POKE 54276,32
8430 RETURN
9999 POKE 214,21: PRINT
```

HILL

```
10 REM        "HILL"
15 DATA 1,9,21,15,3,19,0,7,23,11,5,17,25
20 PRINT CHR$(147);CHR$(18);"{SPC7}PROGR
AMA{SPC}DE{SPC}CIFRADO{SPC}'HILL'{SPC7}"
: CLR
30 POKE 214,2: PRINT: PRINT TAB(2);
   "MODO{SPC}";
40 INPUT M$
50 IF M$="0" THEN 9999
60 IF M$="C" OR M$="D" THEN GOTO 90
70 POKE 214,2: PRINT: PRINT "?";
80 GOTO 30
90 POKE 214,2: PRINT: PRINT "MODO{SPC}:{
SPC}";      M$;"{SPC10}"
100 POKE 214,4: PRINT: PRINT TAB(2);
    "MATRIZ": A=2
104 FOR N=1 TO 4
105 POKE 214,4: PRINT
106 IF N>2 THEN A=26
107 PRINT TAB(A+N*8);
108 INPUT A(N)
109 NEXT
110 A=A(1): B=A(2): C=A(3): D=A(4)
130 L=A*D-B*C
133 GOSUB 1000
137 DET=L
140 IF L<>0 THEN 180
145 PRINT: PRINT: PRINT: PRINT TAB(5);
150 PRINT "NO{SPC}EXISTE{SPC}MATRIZ{SPC}
INVERSA{SPC}PUES{SPC14}EL{SPC}DETERMINAN
TE{SPC}ES{SPC}NULO."
160 PRINT: PRINT:POKE 198,0:
    PRINT "{SPC8}PULSE{SPC}UNA{SPC}TECLA"
170 GET M$: IF M$="" THEN 170
175 GOTO 20
180 IF L/2>INT(L/2) AND L/13>INT(L/13)
    THEN GOTO 210
190 PRINT: PRINT: PRINT:PRINT
    "EL{SPC}DETERMINANTE{SPC}NO{SPC}ES{S
PC}ADECUADO."
200 GOTO 160
210 POKE 214,4: PRINT
211 FOR N=1 TO 79: PRINT "{SPC}";: NEXT
212 POKE 214,4: PRINT
213 PRINT "MATRIZ{SPC}:";TAB(10);A;TAB(1
5);      ",{SPC}";B;TAB(50);C;TAB(55);",{
SPC}";D
220 POKE 214,7: PRINT: PRINT TAB(2);
    "TEXTO:{SPC}";
230 INPUT T$
240 IF T$="0" THEN 9999
260 R$=""
270 FOR I=1 TO LEN(T$)
280 A$=MID$(T$,I,1)
290 IF A$<"A" OR A$>"Z" THEN 310
300 R$=R$+A$
310 NEXT I
320 T$=R$
340 LT=LEN(T$)
350 IF LT>1 THEN 380
360 POKE 214,6: PRINT: PRINT "?":
370 GOTO 220
```

```
380 IF LT/2=INT(LT/2) THEN 410
390 T$=T$+"Z"
400 LT=LT+1
410 POKE 214,7: PRINT: PRINT "TEXTO{SPC}
:{SPC}";     T$;"{SPC30}"
420 IF M$="C" THEN 500
425 FOR I=1 TO 25 STEP 2
426 READ J
427 IF I=DET THEN R=J
428 NEXT I
430 I=A
433 A=D
437 D=I
440 B=-B
445 C=-C
450 L=A*R
453 GOSUB 1000
457 A=L
460 L=B*R
463 GOSUB 1000
464 B=L
465 L=C*R
466 GOSUB 1000
467 C=L
470 L=D*R
473 GOSUB 1000
477 D=L
480 PRINT
490 PRINT "MATRIZ{SPC}MOD.26{SPC}INVERSA
{SPC}:"
491 PRINT
492 PRINT TAB(10);A;TAB(15);",{SPC}";B:
      PRINT TAB(10);C;TAB(15);",{SPC}"
;D
500 PRINT: PRINT : PRINT
510 FOR I=1 TO LT STEP 2
520 L1=ASC(MID$(T$,I,1))-64
530 L2=ASC(MID$(T$,I+1,1))-64
540 L=A*L1+B*L2
550 GOSUB 1000
560 PRINT CHR$(LL+64);
570 L=C*L1+D*L2
580 GOSUB 1000
590 PRINT CHR$(LL+64);
600 NEXT I
610 GOTO 9999
1000 IF L>=0 AND L<26 THEN 1040
1010 IF L<0 THEN L=L+26
1020 IF L>=26 THEN L=L-26
1030 GOTO 1000
1040 LL=L
1050 IF L=0 THEN LL=26
1060 RETURN
9999 POKE 214,21: PRINT: REM END
```

GRONSFELD

```
10 REM        "GRONSFELD"
20 PRINT CHR$(147);CHR$(18);"{SPC5}PROGR
AMA{SPC}DE{SPC}CIFRADO{SPC}'GRONSFELD'{S
PC4}": CLR
30 POKE 214,2: PRINT: PRINT TAB(2);
  "MODO{SPC}Y{SPC}NUMERO{SPC}CLAVE{SPC}";
40 INPUT M$
50 IF M$="0" THEN 9999
60 LM=LEN(M$)
70 IF LM<2 THEN 90
80 M1$=LEFT$(M$,1)
85 IF M1$="C" OR M1$="D" THEN 110
90 POKE 214,2: PRINT: PRINT "?"
100 GOTO 30
110 DIM K(LM-1)
120 FOR I=2 TO LM
130 K$=MID$(M$,I,1)
140 IF K$<"0" OR K$>"9" THEN 20
150 K(I-1)=VAL(K$)
160 NEXT I
170 POKE 214,2: PRINT: PRINT "{SPC}MODO:
{SPC}";      M1$;"{SPC4}NUMERO{SPC}CLAVE:
{SPC}";MID$(M$,2)
180 POKE 214,4: PRINT: PRINT TAB(2);
    "TEXTO{SPC}:";
190 INPUT T$
200 IF T$="0" THEN 9999
210 LT=LEN(T$)
220 IF LT>0 THEN 250
230 POKE 214,4: PRINT: PRINT "?"
240 GOTO 180
250 POKE 214,4: PRINT: PRINT "{SPC}TEXTO
{SPC}:";     T$;"{SPC29}"
260 PRINT
263 CS=ASC("{SPC}")
265 CA=ASC("A")
267 CZ=ASC("Z")
270 IF M1$="D" THEN 370
280 K=0
290 FOR I=1 TO LT
293 IF MID$(T$,I,1)<>"{SPC}" THEN 300
295 L=CS
297 GOTO 340
300 K=K+1
310 IF K=LM THEN K=1
320 L=ASC(MID$(T$,I,1))+K(K)
330 IF L>CZ THEN L=L-26
340 PRINT CHR$(L);
350 NEXT I
360 GOTO 9999
370 K=0
380 FOR I=1 TO LT
383 IF MID$(T$,I,1)<>"{SPC}" THEN 390
385 L=CS
387 GOTO 430
390 K=K+1
400 IF K=LM THEN K=1
410 L=ASC(MID$(T$,I,1))-K(K)
420 IF L<CA THEN L=L+26
430 PRINT CHR$(L);
440 NEXT I
9999 REM END
```

BIFIDO

```
10 REM        "BIFIDO"
20 PRINT CHR$(147);CHR$(18);"{SPC6}PROGR
AMA{SPC}DE{SPC}CIFRADO{SPC}'BIFIDO'{SPC6
}": CLR
30 POKE 214,2: PRINT: PRINT TAB(2);
   "MODO{SPC}Y{SPC}PALABRA{SPC}CLAVE{SPC
}";
40 INPUT M$
60 IF LEN(M$)<2 THEN 80
70 M1$=LEFT$(M$,1)
71 IF M1$="C" OR M1$="D" THEN 100
80 POKE 214,2: PRINT: PRINT "?"
90 GOTO 30
100 DIM A(25)
110 DIM L(25)
115 CA=ASC("A")-1
120 A=0
130 FOR I=2 TO LEN(M$)
140 C=ASC(MID$(M$,I,1))-CA
150 IF L(C)>0 THEN 190
160 A=A+1
170 A(A)=C
180 L(C)=A
190 NEXT I
200 FOR I=1 TO 25
210 IF L(I)>0 THEN 250
220 A=A+1
230 A(A)=I
240 L(I)=A
250 NEXT I
260 POKE 214,2: PRINT:PRINT"MODO:";M1$;"
{SPC39}"
270 POKE 214,4: PRINT:
    PRINT "ALFABETO{SPC}ALTERADO:{SPC}"
280 FOR I=0 TO 4
290 FOR J=1 TO 5
300 POKE 214,4+I: PRINT: PRINT TAB(20+J)
    ;CHR$(A(I*5+J)+CA)
310 NEXT J
320 NEXT I
330 POKE 214,10: PRINT: PRINT
    TAB(2); "LONGITUD{SPC}DEL{SPC}BLOQUE
{SPC}";
340 INPUT B
345 IF B=0 THEN 9999
350 IF B>1 AND B=INT(B) THEN 380
360 POKE 214,10: PRINT: PRINT "?"
370 GOTO 330
380 POKE 214,10: PRINT: PRINT "LONGITUD{
SPC}DEL{SPC}BLOQUE{SPC}:{SPC2}";B;"{SPC1
6}"
385 DIM B(2*B)
390 POKE 214,12: PRINT: PRINT
    TAB(2); "TEXTO{SPC}";
400 INPUT T$
405 IF T$="0" THEN 9999
410 R$=""
420 FOR I=1 TO LEN(T$)
430 A$=MID$(T$,I,1)
440 IF A$>="A" AND A$<="Y" THEN R$=R$+A$
450 NEXT I
460 T$=R$
500 LT=LEN(T$)
510 IF LT>1 THEN 540
520 POKE 214,12: PRINT: PRINT "?"
530 GOTO 390
540 POKE 214,12: PRINT: PRINT "TEXTO:";
    T$;"{SPC23}"
550 PRINT
560 IF M1$="D" THEN 720
570 FOR I=1 TO LT STEP B
580 T=B-1
590 IF I+T>LT THEN T=LT-I
600 FOR J=0 TO T
610 L=ASC(MID$(T$,I+J,1))-CA
620 A=L(L)
630 B(J+1)=INT((A-1)/5)+1
640 B(J+T+2)=A-5*(B(J+1)-1)
650 NEXT J
660 FOR J=0 TO 2*T STEP 2
670 C=(B(J+1)-1)*5+B(J+2)
680 PRINT CHR$(A(C)+CA);
690 NEXT J
700 NEXT I
710 GOTO 9999
720 FOR I=1 TO LT STEP B
730 T=B-1
740 IF I+T>=LT THEN T=LT-I
750 FOR J=0 TO T
760 C=ASC(MID$(T$,I+J,1))-CA
770 A=L(C)
780 B(J*2+1)=INT((A-1)/5)+1
790 B(J*2+2)=A-5*(B(J*2+1)-1)
800 NEXT J
810 FOR J=0 TO T
820 L=(B(J+1)-1)*5+B(J+T+2)
830 PRINT CHR$(A(L)+CA);
840 NEXT J
850 NEXT I
9999 REM END
```

ANALISIS. ¿QUE CIFRADO?

```
10 REM ANALISIS,'QUE CIFRADO ?'
20 PRINT CHR$(147);CHR$(18);"{SPC3}PROGR
AMA{SPC}DE{SPC}ANALISIS{SPC}'QUE{SPC}CIF
RADO'{SPC3}": CLR
30 POKE 214,2: PRINT: PRINT TAB(2);
   "TEXTO{SPC}";
40 INPUT T$
45 IF T$="0" THEN 9999
50 R$=""
60 FOR I=1 TO LEN(T$)
70 A$=MID$(T$,I,1)
80 IF A$>="A" AND A$<="Z" THEN R$=R$+A$
90 NEXT I
100 T$=R$
140 LT= LEN(T$)
150 IF LT>25 THEN 180
160 POKE 214,2: PRINT: PRINT "?"
170 GOTO 30
180 CA=64
190 DIM F(27)
200 FOR I=1 TO LT
210 F(ASC(MID$(T$,I,1))-CA)=
   F(ASC(MID$(T$,I,1))-CA)+1
220 NEXT I
230 M=0
235 OL=0
240 FOR I=1 TO 26
250 IF F(I)>M THEN M=F(I)
255 IF F(I)=0 THEN OL=1
260 NEXT I
270 PRINT CHR$(147)
280 POKE 214,21: PRINT:
290 PRINT TAB(6);
   "--------------------------"
300 PRINT TAB(6);
   "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
310 PRINT TAB(6);
   "--------------------------"
350 FORQ=21TO1STEP-5:POKE211,1:POKE214,Q
:SYS58640:PRINT21-Q"%":NEXTQ
370 FOR I=1 TO 27
373 H=F(I)/LT:IFH=0THEN395
377 IF H>.2 THEN H=.2
378 JJ=100*H
381 POKE211,5+I:POKE214,20-INT(JJ):SYS58
640
382 J=INT((JJ-INT(JJ))*8)
383 IF J=1 THEN PRINT CHR$(164)
384 IF J=2 THEN PRINT CHR$(175)
385 IF J=3 THEN PRINT CHR$(185)
386 IF J=4 THEN PRINT CHR$(162)
387 IF J=5 THEN PRINTCHR$(18);CHR$(184)
388 IF J=6 THEN PRINTCHR$(18);CHR$(183)
389 IF J=7 THEN PRINTCHR$(18);CHR$(163)
390 IFJ=0THENPRINT"{SPC}"
391 FOR J=1 TO INT(JJ)
392 FORQ=1TOI+5:PRINTCHR$(29);:NEXTQ
393 PRINT CHR$(18)"{SPC}"
394 NEXT J
395 NEXTI
400 POKE214,24:POKE211,2:SYS58640:PRINT"
PULSE{SPC}CUALQUIER{SPC}TECLA{SPC}";
401 GETX$:IFX$=""THEN401
410 PRINT CHR$(147)
420 S=0
430 FOR I=1 TO 26
440 S=S+F(I)*(F(I)-1)
450 NEXT I
460 IC=S/(LT*(LT-1))
470 PRINT "INDICE{SPC}DE{SPC}COINCIDENCI
A{SPC}DE{SPC15}LETRAS{SPC}AISLADAS=";IC
480 DIM P(702)
490 LL=LT
500 IF LL/2>INT(LL/2) THEN LL=LL-1
510 FOR I=1 TO LL STEP 2
520 P=(ASC(MID$(T$,I,1))-CA)*26+
      ASC(MID$(T$,I+1,1))-CA
530 P(P)=P(P)+1
540 NEXT I
550 S=0
560 FOR I=1 TO 676
570 S=S+P(I)*(P(I)-1)
580 NEXT I
590 IP=S/(LL*(LL-1))
600 PRINT:PRINT "INDICE{SPC}DE{SPC}COINC
IDENCIA{SPC}DE{SPC}PARES{SPC}DE{SPC6}LET
RAS=";IP
9999 REM END
```

ANALISIS GRONSFELD

```
10 REM ANALISIS 'GRONSFELD'
15 GOSUB 8600
20 PRINT: PRINT "{SPC}POSICIONE{SPC}SU{S
PC}CASSETE{SPC}CON{SPC}EL{SPC}FICHERO{SP
C}DE{SPC2}DATOS."
26 PRINT"{SPC}DESPUES{SPC}PULSE{SPC}CUAL
QUIER{SPC}TECLA."
30 GOSUB 8400: POKE 198,0
40 GET R$: IF R$="" THEN 40
50 GOSUB 5000 : REM LEE FRECUENCIAS
60 GOSUB 6000 : REM LEE TRANSICIONES
65 DIM C(26),P(10,10),K(20),W(15),O(25)
70 PRINT CHR$(147); CHR$(18);
80 PRINT "{SPC4}PROGRAMA{SPC}DE{SPC}ANAL
ISIS{SPC}'GRONSFELD'{SPC4}";
85 PRINT "{SPC40}"
90 POKE 214,2: PRINT:
   PRINT "{SPC2}TEXTO{SPC}";
```

```
100 INPUT T$
105 IF T$="0" THEN 9999
110 R$="": T$=T$+"{SPC}"
120 FOR I=1 TO LEN(T$)
130 IF MID$(T$,I,1)<>"{SPC}" THEN
      R$=R$+MID$(T$,I,1)
140 NEXT I
150 T$=R$
210 LT=LEN(T$)
220 IF LT>10 THEN 250
230 POKE 214,2: PRINT: PRINT "?"
240 GOTO 90
250 POKE 214,2: PRINT: PRINT "TEXTO{SPC}
:{SPC}";    T$;"{SPC30}"
255 CA=64
260 DIM D(LT)
270 F$=""
280 NR=0
290 FOR I=1 TO LT-4
300 J=I+2
305 F=1
310 A$=MID$(T$,I,1): C$=MID$(T$,I+1,1)
311 B$=MID$(T$,J,1): D$=MID$(T$,J+1,1)
312 IF A$<>B$ OR C$<>D$ THEN 400
320 A$=MID$(F$,I,1): C$=MID$(F$,I+1,1)
321 B$=MID$(F$,J,1): D$=MID$(F$,J+1,1)
322 IF A$+B$="**" OR C$+D$="**" THEN 400
330 NR=NR+1
340 D(NR)=J-I
350 F=0
360 S9=I+F: A$="*": GOSUB 8500
370 S9=J+F: A$="*": GOSUB 8500
380 F=F+1
390 IFMID$(T$,I+F,1)=MID$(T$,J+F,1)AND(M
ID$(F$,I+F,1)+MID$(F$,J+F,1))<>"**"THEN3
60
400 J=J+F
410 IF J<=LT-2 THEN 305
420 NEXT I
421 POKE 214,21: PRINT:
    PRINT "{SPC}PULSE{SPC}CUALQUIER{SPC}
TECLA{SPC2}"
422 GET R$
423 IF R$="" THEN 422
424 IF R$="0" THEN 9999
425 IF R$<>"C" THEN 430
426 REM INTRODUZCA AQUI LA RUTINA DE
      IMPRESION
427 GOTO 421
430 PRINT CHR$(147)
431 PRINT "{SPC}HAY";NR;"REPETICIONES"
432 IFNR=0THEN730
440 DATA 2,3,5,7,11,13,17,19,23,29,31
441 DATA 37,41,43,47,53,59,61,67,71,73
442 DATA 79,83,89,97
450 PRINT "{SPC}FACTORES{SPC}DE{SPC}REPE
TICION:"
460 FOR I=1 TO NR
470 R=D(I)
480 PRINT CHR$(18);I;CHR$(146);":{SPC}";
      TAB(4);R;TAB(7);"{SPC}-{SPC}";
490 RESTORE
495 READ P
500 IF R<>2 AND R/2=INT(R/2) THEN 570
510 FOR J=3 TO R-1 STEP 2
520 IF R/J=INT(R/J) THEN 570
530 NEXT J
540 PRINT MID$(STR$(R),2)
550 GOTO 700
560 READ P
570 IF R/P<>INT(R/P) THEN 560
580 PRINT MID$(STR$(P),2);",";
590 R=R/P
600 GOTO 500
700 NEXT I
730 FOR I=1 TO 26: C(I)=0: NEXT
740 FOR I=1 TO LT
750 L=ASC(MID$(T$,I,1))-CA
760 C(L)=C(L)+1
770 NEXT I
780 S=0
790 FOR I=1 TO 26
800 S=S+C(I)*(C(I)-1)
810 NEXT I
820 IC=S/LT/(LT-1)
830 PRINT "{SPC}INDICE{SPC}DE{SPC}COINCI
DENCIA{SPC}:"IC
840 PRINT "{SPC}LONGITUD{SPC}DE{SPC}LA{S
PC}POSIBLE{SPC}CLAVE";
845 INPUT KL
850 IF KL=0 THEN 9999
860 IF KL<2 OR KL>LT/2 OR KL>INT(KL)
    THEN 840
920 PRINT "{SPC}LONGITUD{SPC}DE{SPC}LA{S
PC}CLAVE{SPC}:";KL
930 F$=""
935 FOR I=1 TO 10: FOR J=1 TO 10:
936 P(I,J)=0
937 K(I+J-1)=-1
938 NEXT J
939 NEXT I
940 FOR I=1 TO 26
950 C(I)=C(I)/LT
960 NEXT I
961 PRINT "{SPC}PULSE{SPC}CUALQUIER{SPC}
TECLA{SPC}"
962 GET R$
963 IF R$="" THEN 962
964 IF R$="C" THEN REM LLAME A LA RUTINA
    DE IMPRESION
965 PRINT CHR$(147)
969 GOTO 7000
970 FOR C=1 TO KL
980 GOSUB 8000
990 NEXT C
1140 NC=0
1150 NC=NC+1
1160 IF LT/NC/KL>15 THEN 1150
1165 CL=NC*KL
1167 NR=LT/CL
1170 PRINTCHR$(19)
1171 FORI=0 TO NC-1
1180 FOR J=1 TO KL
1190 POKE214,0:PRINT:PRINTTAB(I*KL+J);
1195 PRINTMID$(STR$(J),2,1)
1200 NEXT J
1210 NEXT I
1260 GOSUB 8200
1270 POKE 214,21: PRINT: PRINT "PULSE{SP
C}A,B,C,D,E,F,K,N,P,S,T,W,0{SPC}"
1280 GET R$
1290 IF R$="" THEN 1280
```

```
1295 FORI=15 TO 22
1296 POKE214,I:PRINT:PRINT"{SPC38}"
1297 NEXTI
1300 POKE 214,21: PRINT: PRINT "{SPC32}"
1305 IF R$="A" THEN 7000
1310 IF R$<>"B" THEN 1380
1320 GOSUB 8300
1330 K(C)=-1
1333 FOR I=1 TO 10
1335 P(C,I)=0
1337 NEXT I
1340 FOR I=C TO LT STEP KL
1350 A$="{SPC}": S9=I: GOSUB 8500
1360 NEXT I
1370 GOTO 1260
1380 IF R$<>"C" THEN 1410
1385 POKE211,1:POKE214,23:SYS58640:PRINT
"CONSULTE{SPC}EL{SPC}APENDICE"
1390 REM RUTINA DE IMPRESION
1400 GOTO 1270
1410 IF R$<>"D" THEN 1450
1415 F$=""
1420 FOR I=1 TO LT:F$=F$+"{SPC}":NEXT I
1430 FOR I=1 TO KL
1431 K(I)=-1
1432 NEXT I
1435 FOR I=1 TO 10: FOR J=1 TO 10:
1436 P(I,J)=0
1437 NEXT J,I
1440 GOTO 1260
1450 IF R$<>"E" THEN 1500
1460 POKE211,1:POKE214,23:SYS58640:INPUT
 "LETRA{SPC}";L$
1465 IF L$="0" THEN 9999
1470 IF LEN(L$)<>1 OR L$<"A" OR L$>"Z"
     THEN 1460
1480 POKE 214,20: PRINT: PRINT "{SPC39}"
1481 POKE 214,22: PRINT: PRINT TAB(12);
L$;":";       E(ASC(L$)-CA)
1490 GOTO 1270
1500 IF R$<>"F" THEN 1550
1505 Z=-2
1510 FOR C=1 TO KL
1520 IF K(C)>=0 THEN 1530
1525 IF (MID$(F$,KL+C-1,1)<>"{SPC}")+(MI
D$(F$,C+1,1)<>"{SPC}")=Z THEN GOSUB 8000
:GOSUB 8200
1530 NEXT C
1533 Z=Z-1
1536 IF Z>=0 THEN 1510
1537 FOR I=1 TO KL
1538 IF K(I)<0 THEN 1505
1539 NEXT I
1540 GOTO 1260
1550 IF R$<>"K" THEN 1580
1560 PRINT CHR$(147)
1570 GOTO 840
1580 IF R$<>"N" THEN 1620
1590 GOSUB 8300
1600 GOSUB 8000
1610 GOTO 1260
1620 IF R$="P" THEN 7230
1625 IF R$<>"S" THEN 1660
1630 PRINT CHR$(147)
1631 PRINT "CLAVE{SPC}:{SPC}";
1632 FOR I=1 TO KL
1633 PRINT K(I);
1634 NEXT I
1640 PRINT: PRINT F$
1650 GOTO 9999
1660 IF R$<>"T" THEN 1740
1670 POKE211,1:POKE214,23:SYS58640:INPUT
 "LETRAS{SPC}";L$
1680 IF L$="0" THEN 9999
1681 IF LEN(L$)<>2 THEN 1670
1690 L1=ASC(LEFT$(L$,1))-CA
1700 L2=ASC(RIGHT$(L$,1))-CA
1710 IF L1<1 OR L1>26 OR L2<1 OR L2>26
     THEN 1670
1720 POKE 214,20: PRINT: PRINT "{SPC39}"
1721 POKE 214,22: PRINT: PRINT TAB(14);L
$;":";T(L1,L2)
1730 GOTO 1270
1740 IF R$<>"W" THEN 1800
1750 GOSUB 8300
1760 POKE211,0:POKE214,23:SYS58640:INPUT
 "{SPC5}CLAVE{SPC3}";D
1770 IF D<0 OR D>9 OR D>INT(D) THEN 1760
1780 GOSUB 8170
1790 GOTO 1260
1800 IF R$="0" THEN 9999
1810 POKE 214,21: PRINT: PRINT "?"
1820 GOSUB 8400
1830 GOTO 1270
5000 DIM E(26)
5010 OPEN 1,1,0,"FRECUENCIAS"
5020 FOR I=1 TO 26
5030 INPUT#1,E(I)
5040 NEXT I
5050 CLOSE 1
5060 RETURN
6000 DIM T(26,26)
6010 OPEN 1,1,0,"TRANSICIONES"
6020 FOR I=1 TO 26
6030 FOR J=1 TO 26
6040 INPUT#1,T(I,J)
6050 NEXT J
6060 NEXT I
6070 CLOSE 1
6080 RETURN
7000 PRINT "PALABRA{SPC}PROBABLE{SPC}";:
 INPUT W$
7010 IF W$="0" THEN 9999
7020 IF W$="" THEN 970
7030 LW=LEN(W$)
7050 FOR I=1 TO LW
7060 W(I)=ASC(MID$(W$,I,1))-CA
7065 IF W(I)<1 OR W(I)>26 THEN 7000
7070 NEXT I
7080 NP=0
7100 FOR I=0 TO LT-LW-1
7110 FOR J=1 TO LW
7120 L=ASC(MID$(T$,I+J,1))-CA
7130 FOR K=0 TO 9
7140 N=L-K
7150 IF N<1 THEN N=N+26
7160 IF N=W(J) THEN 7190
7170 NEXT K
7180 GOTO 7220
7190 NEXT J
7200 NP=NP+1
7210 O(NP)=I+1
```

```
7220 NEXT I
7230 PRINT CHR$(147)
7235 IF NP>0 THEN 7260
7240 PRINT CHR$(34);W$;CHR$(34);
     "NO{SPC}PUEDE{SPC}SER."
7250 GOTO 7000
7260 PRINT "PUEDE{SPC}ESTAR{SPC}EN";NP;"
SITIOS:"
7270 FOR I=1 TO NP
7280 PRINT CHR$(18);I;CHR$(146);":";
     O(I);"-"
7290 FOR J=0 TO LW-1
7300 PRINT MID$(T$,J+O(I),1);
7310 NEXT J
7320 PRINT
7330 NEXT I
7335 F$=T$
7340 PRINT "NUMERO{SPC}DE{SPC}LA{SPC}OPC
ION{SPC}QUE{SPC}ESCOGE{SPC}";:INPUT O
7345 IF O=0 THEN 9999
7350 IF O<1 OR O>NP OR O>INT(O)
     THEN 7340
7360 P=O(O)
7370 C=P-KL*INT(P/KL)
7380 IF C=0 THEN C=KL
7390 FOR J=0 TO LW-1
7400 L=ASC(MID$(T$,P+J,1))-CA
7410 FOR K=0 TO 9
7420 N=L-K
7430 IF N<1 THEN N=N+26
7440 IF N<>W(J+1) THEN NEXT K
7450 D=K
7455 GOSUB 8170
7460 C=C+1
7470 IF C>KL THEN C=C-KL
7480 NEXT J
7490 PRINT CHR$(147)
7500 GOTO 1140
8000 B=999
8005 D=0
8010 FOR K=0 TO 9
8020 IF P(C,K+1)<>0 THEN 8160
8030 T=0
8040 N=L-K
8050 IF N<1 THEN N=N+26
8060 T=T+(LT/KL)*ABS(E(N)-C(L))
8065 FOR J=0 TO LT-KL STEP KL
8070 P=C+J
8080 L=ASC(MID$(T$,P,1))-CA
8100 IF P<=1 THEN 8110
8102 IF MID$(F$,P-1,1)="{SPC}" THEN 8110
8104 T=T-T(ASC(MID$(F$,P-1,1))-CA,N)
8110 IF P>=LT THEN 8120
8112 IF MID$(F$,P+1,1)="{SPC}" THEN 8120
8114 T=T-T(N,ASC(MID$(F$,P+1,1))-CA)
8120 NEXT J
8130 IF T>B THEN 8160
8140 B=Y
8150 D=K
8160 NEXT K
8170 K(C)=D
8175 P(C,D+1)=1
8180 FOR I=C TO LT STEP KL
8182 L=ASC(MID$(T$,I,1))-CA-D
8184 IF L<1 THEN L=L+26
8186 A$=CHR$(L+CA):S9=I: GOSUB 8500
8188 NEXT I
8190 RETURN
8200 FOR I=0 TO NR-1
8210 POKE 214,2+I:PRINT:PRINTTAB(1): PRI
NT MID$(F$,CL*I+1,CL)
8220 NEXT I
8225 IFLT/CL>INT(LT/CL)THENPOKE214,2+I:P
RINT:PRINTTAB(1):PRINTMID$(F$,CL*I+1)
8230 FOR I=0 TO NC-1
8240 FOR J=1 TO KL
8250 POKE 214,4+INT(NR+(NR>INT(NR))):
     PRINT: PRINT TAB(I*KL+J);
8255 PRINT MID$(STR$(K(J)),2,1)
8260 NEXT J
8270 NEXT I
8280 RETURN
8300 POKE211,1:POKE214,23:SYS58640:PRINT
 "QUE{SPC}COLUMNA{SPC}";: INPUT C
8310 IF C=0 THEN 9999
8320 IF C<1 OR C>KL OR C>INT(C)
     THEN 8300
8330 RETURN
8400 POKE 54276,33
8410 FOR S9=0 TO 500:NEXT
8420 POKE 54276,32
8430 RETURN
8500 F$=LEFT$(F$,S9-1)+A$+MID$(F$,S9+1):
     RETURN
8600 POKE 53280,0: POKE 53281,7:
8610 POKE 646,0: PRINTCHR$(147)
8620 FOR I=54272 TO 54295: POKE I,0:NEXT
8630 POKE 54272,200: POKE54273,100
8640 POKE 54277,0  : POKE54278,128
8650 POKE 54276,32 : POKE54296,15
8660 RETURN
9999 POKE 214,21: PRINT:
     REM END
```

SEGURO

```
10 REM          'SEGURO'
20 PRINT CHR$(147);CHR$(18);"{SPC3}PROGR
AMA{SPC}DE{SPC}CIFRADO{SPC4}'SEGURO'{SPC
6}": CLR
30 POKE 214,2: PRINT: PRINT TAB(2);
   "MODO{SPC}";
40 INPUT M$
50 IF M$="0" THEN 835
60 IF M$="C" OR M$="D" THEN 90
70 POKE 214,2: PRINT: PRINT "?";
80 GOTO 30
90 POKE 214,2: PRINT: PRINT TAB(2);
```

```
   "MODO{SPC}:{SPC}";M$
95 DIM K(5)
100 POKE 214,4: PRINT: PRINT TAB(2);
    "INTRODUZCA{SPC}5{SPC}NUMEROS{SPC}EN
TRE{SPC}1{SPC}Y{SPC}256"
101 PRINT"{SPC2}PARA{SPC}COLOCARLOS{SPC}
COMO{SPC}SEMILLA."
105 FOR S=1 TO 5
110 INPUT K(S)
120 IF K(S)=0  THEN 835
130 IF K(S)>0 AND K(S)<256 AND K(S)=INT(
K(S)) THEN 155
140 POKE 214,4: PRINT: PRINT "?";
150 GOSUB 8000:GOTO 100
155 NEXT S
156 GOSUB 8000
160 POKE 214,4: PRINT: PRINT TAB(2); "NU
MERO{SPC}CLAVE{SPC}:";K(1);K(2);K(3);K(4
);K(5)
170 POKE 214,6: PRINT: PRINT TAB(2);
    "PALABRA{SPC}CLAVE{SPC}";
180 INPUT K$
190 IF K$="0" THEN 835
200 LK= LEN(K$)
210 IF LK>0 THEN 240
220 POKE 214,6: PRINT: PRINT "?"
230 GOTO 170
240 DIM A(25):REM ALFABETO ALTERADO DE 2
5 LETRAS.NO SE ADMITE LA Z.
250 DIM L(25)
260 CA=64
270 A=0
280 FOR I=1 TO LK
290 C=ASC(MID$(K$,I,1))-CA
300 IF C<1 OR C>25 THEN 220
310 IF L(C)>0 THEN 350
320 A=A+1
330 A(A)=C
340 L(C)=A
350 NEXT I
360 FOR I=1 TO 25
370 IF L(I)>0 THEN 410
380 A=A+1
390 A(A)=I
400 L(I)=A
410 NEXT I
420 POKE 214,6: PRINT:
    PRINT "{SPC2}ALFABETO{SPC}ALTERADO:{
SPC}";
430 FOR I=0 TO 4
440 FOR J=1 TO 5
450 POKE 214,6+I: PRINT: PRINT
    TAB(20+J);CHR$(A(I*5+J)+CA)
460 NEXT J
470 NEXT I
480 POKE 214,12: PRINT:
    PRINT TAB(2);"TEXTO{SPC}";
490 INPUT T$
500 IF T$="0" THEN 835
510 R$=""
520 FOR I=1 TO LEN(T$)
530 A$=MID$(T$,I,1)
540 IF A$>="A" AND A$<="Z" THEN R$=R$+A$
550 NEXT I
560 T$=R$
600 LT=LEN(T$)
610 IF LT>0 THEN 640
620 POKE 214,12: PRINT: PRINT "?"
630 GOTO 480
640 POKE 214,12: PRINT: PRINT "TEXTO{SPC
}:";T$;"{SPC8}"
650 POKE139,K(1):POKE140,K(2):
    POKE141,K(3)
655 POKE142,K(4):POKE143,K(5)
660 IF M$="D" THEN 760
670 FOR I=1 TO LT
680 C=ASC(MID$(T$,I,1))-CA
690 X=INT((C-1)/5)+INT(RND(1)*5)+2
700 IF X>5 THEN X=X-5
710 Y=C-INT((C-1)/5)*5+INT(RND(1)*5)+1
720 IF Y>5 THEN Y=Y-5
730 PRINT CHR$(L((X-1)*5+Y)+CA);
740 NEXT I
750 GOTO 835
760 FOR I=1 TO LT
770 C=A(ASC(MID$(T$,I,1))-CA)
780 X=INT((C-1)/5)-INT(RND(1)*5)
790 IF X<1 THEN X=X+5
800 Y=C-INT((C-1)/5)*5-INT(RND(1)*5)-1
810 IF Y<1 THEN LET Y=Y+5
820 PRINT CHR$((X-1)*5+Y+CA);
830 NEXT I
835 END
8000 FOR B=1184 TO 1503:POKEB,32:NEXT B
8010 RETURN
```

CREACION DE DATOS

```
5 PRINTCHR$(147)
10 PRINT CHR$(18);TAB(5);"PROGRAMA{SPC}D
E{SPC}CREACION{SPC}DE{SPC}DATOS"    :PRIN
T
20 PRINT "ESCRIBA{SPC}LA{SPC}FRECUENCIA{
SPC}PARA{SPC}CADA{SPC}LETRA{SPC3}SEGUN{S
PC}SE{SPC}PIDA"
30 DIM E(26)
40 FOR I=1 TO 26
50 PRINT CHR$(64+I);
60 INPUT E(I)
70 NEXT
80 PRINT "INTRODUZCA{SPC}LA{SPC}CINTA{SP
C}PARA{SPC}ALMACENAR{SPC}ESTE{SPC}FICHER
O{SPC}Y{SPC}POSICIONELA"
90 FOR I=1 TO 5000: NEXT
100 PRINT: PRINT "{SPC}DESPUES{SPC}PULSE
{SPC}CUALQUIER{SPC}TECLA."
110 POKE 198,0
120 GET A$: IF A$="" THEN 120
```

```
130 OPEN 1,1,1,"FRECUENCIAS"
140 FOR I=1 TO 26
150 PRINT#1,E(I)
160 NEXT
170 CLOSE 1
180 PRINT
190 PRINT "ESCRIBA{SPC}AHORA{SPC}LOS{SPC
}DATOS{SPC}DE{SPC}TRANSICION{SPC}PARA{SP
C}CADA{SPC}PAR{SPC}DE{SPC}LETRAS"
200 DIM T(26,26)
210 FOR I=1 TO 26
220 FOR J=1 TO 26
230 PRINT CHR$(64+I);CHR$(64+J);
240 INPUT T(I,J)
250 NEXT J
260 NEXT I
270 PRINT "INTRODUZCA{SPC}LA{SPC}CINTA{S
PC}PARA{SPC}ALMACENAR{SPC}ESTE{SPC}FICHE
RO{SPC}Y{SPC}POSICIONELA"
280 FOR I=1 TO 5000: NEXT
290 PRINT: PRINT "{SPC}DESPUES{SPC}PULSE
{SPC}CUALQUIER{SPC}TECLA."
300 POKE 198,0
310 GET A$: IF A$="" THEN 310
320 OPEN 1,1,1,"TRANSICIONES"
330 FOR I=1 TO 26
340 FOR J=1 TO 26
350 PRINT#1,T(I,J)
360 NEXT J,I
370 CLOSE 1
380 PRINT
390 PRINT "TODO{SPC}LISTO{SPC}!"
```

Programas para Apple II

CESAR

```
10  REM  *********
11  REM     CESAR
12  REM  *********
13  HOME
15  DIM M$(2)
16 YA = 0:C$ = ""
20  HTAB 3: VTAB 2: PRINT "PROGRA
     MA DE CIFRADO 'CESAR'"
21  PRINT "  --------------------
     -------"
30  HTAB 4: VTAB 10
40  PRINT "MODO : ";
50  INPUT "";M$(1)
52  PRINT : PRINT "   CLAVE : ";
55  INPUT "";M$(2)
60  IF M$(1) = "0" THEN  GOTO 999
     9
70  IF M$(1) < "C" OR M$(1) > "D"
      THEN  GOTO 100
80  IF M$(2) < "A" OR M$(2) > "Z"
      THEN  GOTO 100
90  GOTO 120
100  PRINT : PRINT "? ";
110  GOTO 40
120  VTAB 5: HTAB 4: PRINT "MODO
     : ";M$(1);"   CLAVE : ";M$(2
     )
125  FOR H = 1 TO 500: NEXT H
130 K =  ASC (M$(2)) -  ASC ("A")

133  POKE 34,6
135  HOME
140  VTAB 7: HTAB 5: PRINT "TEXTO
      : ";
150  INPUT "";T$
155  POKE 34,9
170  IF M$(1) = "C" THEN  GOTO 19
     0
180 K =  - K
190 L =  LEN (T$)
195  VTAB 12: PRINT
200  FOR I = 1 TO L
220 C$ =  RIGHT$ ( LEFT$ (T$,I),1
     )
225  IF C$ = "0" AND YA = 0 THEN
      GOTO 9999
226 YA = 1
230  IF  ASC (C$) >  = 65 AND  ASC
```

```
    (C$) <  = 90 THEN  GOTO 250
235  PRINT " ";
240  GOTO 280
250 W =  ASC (C$) -  ASC ("A") +
    K
260  GOSUB 420
270  PRINT  CHR$ (W +  ASC ("A"))
    ;
280  NEXT I
290  IF M$(1) = "C" THEN  GOTO 99
    99
300  VTAB 23: HTAB 1: PRINT "PULS
    A 'S' PARA SEGUIR, 'N' PARA
    ACABAR"
310  INPUT "";IN$
320  IF IN$ <  > "S" AND IN$ <  >
    "N" THEN  GOTO 310
330  IF IN$ = "" THEN  GOTO 320
340  IF IN$ = "N" THEN  GOTO 9999

350  IF IN$ = "S" THEN  HOME : GOTO
    380
360  PRINT : PRINT "? ";
370  GOTO 310
380 W = 1 - K
385 W = 1 - K
390  GOSUB 420
400 K =  - W
410  GOTO 195
420  IF W <  = 25 THEN  GOTO 440
430 W = W - 26
440  IF W >  = 0 THEN  GOTO 460
450 W = W + 26
460  RETURN
9999  POKE 34,0: END : REM  FIN
```

MONO

```
10  REM   ********
11  REM      MONO
12  REM   ********
13  HOME
20  PRINT : HTAB 4: PRINT "PROGRA
     MA DE CIFRADO MONOALFABETICO
     "
21  HTAB 4: PRINT "-------------
     --------------------"
25  DIM M$(2),C2$(100)
30  VTAB 9: HTAB 4
40  PRINT "MODO : ";
41  INPUT "";M$(1)
42  IF M$(1) = "O" THEN  GOTO 999
     9
43  PRINT : HTAB 4: PRINT "MEZCLA
      : ";
44  INPUT "";M$(2)
45  PRINT : HTAB 4: PRINT "CLAVE
     : ";
46  INPUT "";CL$
90  IF M$(1) < "C" OR M$(1) > "D"
      THEN  GOTO 150
100  IF M$(2) < "S" OR M$(2) > "T
    " THEN  GOTO 150
120  FOR I = 1 TO  LEN (CL$)
121 C1$ =  MID$ (CL$,I,1)
122  IF C1$ < "A" OR C1$ > "Z" THEN
     GOTO 150
130  NEXT I
131  POKE 34,3: HOME
132  VTAB 6: HTAB 5: PRINT "MODO
    = ";M$(1);"              ";
134  PRINT "MEZCLA = ";M$(2)
136  PRINT : HTAB 10: PRINT "CLAV
    E : ";CL$
137 B =  LEN (CL$)
140  GOTO 220
150  PRINT
160  IF M$(1) <  > "C" AND M$(1) <
      > "D" THEN  HTAB 5: PRINT "
    SOLO HAY DOS MODOS ": PRINT
    : HTAB 10: PRINT "C - CIFRAD
    O     D - DESCIFRADO"
170  IF M$(2) <  > "S" AND M$(2) <
      > "T" THEN  PRINT : PRINT "
    DOS TIPOS DE MEZCLA  'S' Y '
    T'"
180  PRINT : PRINT "LA CLAVE ES U
    NA PALABRA COMPUESTA SOLO": PRINT
    : PRINT "POR LETRAS. NO SE A
    DMITEN OTROS SIMBOLOS"
190  GOTO 30
220 LJ =  LEN (CL$):CL$ = CL$ + "
    ABCDEFGHIJKLMNOPQRSTUVWXYZ"
230 LI =  LEN (CL$)
240 C$ = ""
250 CA =  ASC ("A") - 1
260  DIM A$(26)
270  FOR I = 1 TO LI
275 C1$ =  MID$ (CL$,I,1)
280 AS =  ASC (C1$) - CA
290  IF A$(AS) <  > "" THEN  GOTO
    310
300 C$ = C$ + C1$
310  IF I <  > LJ THEN  GOTO 330
320 B =  LEN (C$)
330 A$(AS) = "*"
340  NEXT I
350  IF M$(2) = "S" THEN  GOTO 56
    0
360 D =  INT (26 / B)
```

```
361 LC = B * D
362  IF LC = 26 THEN  GOTO 430
364 D = D + 1
365 LC = B * D
400  FOR I = 27 TO LC
410 C$ = C$ + "*"
420  NEXT I
430  DIM B$(D,B)
435 W = 1
440  FOR J = 1 TO D
450  FOR I = 1 TO B
460 B$(J,I) =  MID$ (C$,W,1)
465 W = W + 1
470  NEXT
480  NEXT
490 C$ = ""
500  FOR I = 1 TO B
510  FOR J = D TO 1 STEP  - 1
520  IF B$(J,I) = "*" THEN  GOTO
     540
530 C$ = C$ + B$(J,I)
540  NEXT J
550  NEXT I
560  REM  M$(2)="S"
600  VTAB 10: PRINT "TEXTO : ";
610  INPUT "";T$
620  VTAB 11: PRINT "          ";
630  IF T$ = "0" THEN  GOTO 9999
640 LT =  LEN (T$)
650  IF M$(1) = "C" THEN  GOTO 73
     0
660  DIM P$(26)
670  FOR I = 1 TO 26
680 P$( ASC ( MID$ (C$,I,1)) - CA
     ) =  CHR$ (CA + I)
690  NEXT I
700 C$ = ""
705  FOR I = 1 TO 26
710 C$ = C$ + P$(I)
720  NEXT
730  FOR I = 1 TO LT
735 T1$ =  MID$ (T$,I,1)
740  IF T1$ < "A" OR T1$ > "Z" THEN
      GOTO 770
750  PRINT  MID$ (C$, ASC (T1$) -
     CA,1);
760  GOTO 780
770  PRINT " ";
780  NEXT I
9999  POKE 34,1: REM  FIN
```

PROGRAMA DE ANALISIS DE FRECUENCIAS

```
10  REM  PROGRAMA DE ANALISIS DE
     FRECUENCIA
15  HOME
20  PRINT "PROGRAMA DE ANALISIS D
     E FRECUENCIA "
21  PRINT "----------------------
     -------------"
30  HTAB 3: VTAB 3: PRINT "TEXTO:
      ";
40  INPUT "";T$
50  IF T$ = "0" THEN  GOTO 9999
60  FOR I = 1 TO  LEN (T$)
70  IF I >  LEN (T$) THEN  GOTO 1
     40
80  IF  MID$ (T$,I,1) >  = "A" AND
      MID$ (T$,I,1) <  = "Z" THEN
      GOTO 140
90 R$ = ""
100  IF I > 1 THEN R$ =  LEFT$ (T
     $,I - 1)
110  IF I <  LEN (T$) THEN R$ = R
     $ +  RIGHT$ (T$, LEN (T$) -
     I)
120 T$ = R$
130  GOTO 70
140  NEXT I
150 LT =  LEN (T$)
160  IF LT > 3 THEN  GOTO 190
170  HTAB 1: VTAB 3: PRINT "?"
180  GOTO 40
190  PRINT : PRINT : PRINT "TEXTO
      : ";T$
200  GOSUB 8000
210 CA =  ASC ("A") - 1
220  DIM E(26)
230  PRINT "FRECUENCIAS TELATIVAS
     :"
240  FOR I = 1 TO LT
250 E( ASC ( MID$ (T$,I,1)) - CA)
      = E( ASC ( MID$ (T$,I,1)) -
     CA) + 1
260  NEXT I
270  FOR I = 1 TO 26
275  HTAB 1: IF I / 2 =  INT (I /
     2) THEN  HTAB 20
276  VTAB 5 +  INT (I / 2 + .5)
280  INVERSE : PRINT  CHR$ (I + C
     A);: NORMAL : PRINT ": ";E(I
     ) / LT,
290  NEXT I
300  GOSUB 8000
310  DIM D(26)
320  FOR I = 1 TO LT - 1
330  IF  MID$ (T$,I,1) =  MID$ (T
```

```
$,I + 1,1) THEN D( ASC ( MID$
(T$,I,1)) - CA) = D( ASC ( MID$
(T$,I,1)) - CA) + 1
340  NEXT I
350  PRINT "LETRAS REPETIDAS : "
360  FOR I = 1 TO 26
365  HTAB 1: IF I / 2 =  INT (I /
2) THEN  HTAB 20
366  VTAB 5 +  INT (I / 2 + .5)
370  INVERSE : PRINT  CHR$ (I + C
A); CHR$ (I + CA);: NORMAL :
 PRINT ": ";D(I),
380  NEXT I
390  GOSUB 8000
400  PRINT "FRECUENCIAS ABSOLUTAS
 DE DIGRAMAS:"
410  DIM T(26,26)
420  FOR I = 1 TO LT - 1
430 T( ASC ( MID$ (T$,I,1)) - CA,
 ASC ( MID$ (T$,I + 1,1)) -
CA) = T( ASC ( MID$ (T$,I,1)
) - CA, ASC ( MID$ (T$,I + 1
,1)) - CA) + 1
440  NEXT I
450  FOR I = 1 TO 26
460  FOR J = 1 TO 26
470  IF T(I,J) > 0 THEN  INVERSE
: PRINT  CHR$ (I + CA); CHR$
(J + CA);: NORMAL : PRINT ":
 ";T(I,J),
480  IF  PEEK ( - 16384) > 127 THEN
 GOSUB 8000
490  NEXT J
500  NEXT I
510  GOSUB 8000
515  DIM F(26,26)
520  PRINT "DATOS INVERSOS : "
530  FOR I = 1 TO 26
540  FOR J = 1 TO 26
550  IF T(I,J) > 0 AND T(J,I) > 0
 AND I <  > J AND F(I,J) = 0
 AND F(J,I) = 0 THEN  INVERSE
: PRINT  CHR$ (I + CA); CHR$
(J + CA);: NORMAL : PRINT ":
 ";T(I,J),: INVERSE : PRINT
 CHR$ (J + CA); CHR$ (I + CA
);: NORMAL : PRINT ": ";T(J,
I):F(I,J) = 1
560  IF  PEEK ( - 16384) > 127 THEN
 GOSUB 8000
570  NEXT J
580  NEXT I
590  GOSUB 8000
600  DIM R(26,26)
610  FOR I = 1 TO 26
620  IF E(I) = 0 THEN  GOTO 660
630  FOR J = 1 TO 26
640 R(I,J) = T(I,J) / E(I)
650  NEXT J
660  NEXT I
670  PRINT "PROBABILIDAD DERECHA:
 "
671 W = 1
680  FOR I = 1 TO 26
690  FOR J = 1 TO 26
698  HTAB 1: IF W / 2 =  INT (W /
2) THEN  HTAB 20
699  VTAB 5 +  INT (W / 2 + .5)
700  IF R(I,J) > 0 THEN  INVERSE
: PRINT  CHR$ (I + CA); CHR$
(J + CA);: NORMAL : PRINT ":
 ";R(I,J):W = W + 1: IF W =
61 THEN W = 1
710  IF  PEEK ( - 16384) > 127 THEN
 GOSUB 8000
720  NEXT J
730  NEXT I
740  GOSUB 8000
750  DIM L(26,26)
760  FOR I = 1 TO 26
770  IF E(I) = 0 THEN  GOTO 810
780  FOR J = 1 TO 26
790 L(I,J) = T(J,I) / E(I)
800  NEXT J
810  NEXT I
820  PRINT "PROBABILIDAD IZQUIERD
A : "
821 W = 1
830  FOR I = 1 TO 26
840  FOR J = 1 TO 26
845  HTAB 1: IF W / 2 =  INT (W /
2) THEN  HTAB 20
846  VTAB 5 +  INT (W / 2 + .5)
850  IF L(I,J) > 0 THEN  INVERSE
: PRINT  CHR$ (J + CA); CHR$
(I + CA);: NORMAL : PRINT ":
 ";L(I,J):W = W + 1: IF W =
61 THEN W = 1
860  IF  PEEK ( - 16384) > 127 THEN
 GOSUB 8000
870  NEXT J
880  NEXT I
890  GOSUB 8000
900  DIM G(26,LT)
910  FOR I = 1 TO 26
920  FOR J = 2 TO LT - 1
930  IF  MID$ (T$,J,1) =  CHR$ (I
 + CA) THEN G(I,J) = 1
940  NEXT J
950  NEXT I
960  PRINT "TRIGRAMAS: "
970  FOR I = 1 TO 26
980  IF E(I) = 0 OR (E(I) = 1 AND
( MID$ (T$,1,1) =  CHR$ (I +
CA) OR  MID$ (T$,LT,1) =  CHR$
(I + CA))) THEN  GOTO 1050
990  INVERSE : PRINT  CHR$ (I + C
A);: NORMAL : PRINT ": ";
1000  FOR J = 2 TO LT
1010  IF G(I,J) = 1 THEN  PRINT  MID$
(T$,J - 1,3);", ";
1020  NEXT J
1030  PRINT  CHR$ (8);" "
1040  IF  PEEK ( - 16384) > 127 THEN
 GOSUB 8000
1050  NEXT I
```

```
1060  GOSUB 8000
1070  GOTO 9999
8000  PRINT : PRINT : PRINT
8005  HTAB 1: VTAB 22: PRINT "PUL
      SA UNA TECLA "
8010  GET R$
8060  IF R$ = "0" THEN  GOTO 9999

8070  HOME
8080  RETURN
9999  REM  FIN
```

AYUDA MONOALFABETICA

```
5  DIM E(26),T(26,26),N(26)
10  REM  AYUDA MONOALFABETICA
20  PRINT "INTRUDUZCA UN DISCO CO
     N DATOS Y          PULSE UNA
     TECLA"
25  GET A$
26  PRINT : PRINT
28  PRINT  CHR$ (4);"OPEN FRECUEN
     CIA"
30  PRINT  CHR$ (4);"READ FRECUEN
     CIA"
32  FOR I = 1 TO 26
34  INPUT E(I):E(I) = E(I) / 100
36  NEXT
38  PRINT  CHR$ (4)"CLOSE FRECUEN
     CIA"
40  PRINT  CHR$ (4);"OPEN TRANSIC
     ION"
42  PRINT  CHR$ (4);"READ TRANSIC
     ION"
44  FOR I = 1 TO 26
46  FOR J = 1 TO 26
48  INPUT T(I,J):T(I,J) = T(I,J) /
     100
50  NEXT : NEXT
52  PRINT  CHR$ (4)"CLOSE TRANSIC
     ION"
70  HOME
80  PRINT "PROGRAMA DE AYUDA MONO
     ALFABETICA"
90  INPUT "TEXTO: ";T$
110  IF  LEFT$ (T$,1) = "0" THEN
      GOTO 9999
120 LT =  LEN (T$)
130  IF LT > 9 THEN  GOTO 160
140  PRINT "TEXTO CORTO"
150  GOTO 70
160  DIM T$(LT): FOR I = 1 TO LT:
     T$(I) =  MID$ (T$,I,1): NEXT

165  FOR I = 1 TO LT
180  IF T$(I) < "A" OR T$(I) > "Z
     " THEN T$(I) = " "
200  NEXT I
230  GOSUB 8300
232  PRINT "TEXTO: ";T$
234 BL = 6 +  INT ((LT - 1) / 15)

236  DIM C(26)
238 CA =  ASC ("A") - 1
240  FOR I = 1 TO LT
245  IF T$(I) <  > " " THEN C( ASC
     (T$(I)) - CA) = C( ASC (T$(I
     )) - CA) + 1 / LT
250  NEXT I
260  GOSUB 8000
265  HOME
270  FOR I = 1 TO 26
280  PRINT  CHR$ (I + CA);": "; INT
     (1000 * C(I) + .5) / 10,
290  NEXT I
300  GOSUB 8000
310  DIM A$(26),B$(26),P$(LT)
315  FOR I = 1 TO 26:A$(I) = "*":
     B$(I) = "*": NEXT
320  HOME
380  HTAB 1: VTAB 4: PRINT "ABCDE
     FGHIJKLMNOPQRSTUVWXYZ"
381  HTAB 1: VTAB 5: FOR X = 1 TO
     26: PRINT A$(X);: NEXT : PRINT

385 P$ = ""
390  FOR I = 0 TO 15 *  INT ((LT -
     1) / 15) STEP 15
400 J = 15
410  IF I + J > LT THEN J = LT -
     I
415  GOSUB 8300
420  PRINT : PRINT  MID$ (T$,I +
     1,J); TAB( 18);"-";
430  FOR W = 1 TO J
440  LET C$ = " "
450  IF T$(I + W) <  > " " THEN C
     $ = A$( ASC (T$(I + W)) - CA)
460 P$(I + W) = C$
470  PRINT C$;
480  NEXT W
490  NEXT I
500  HTAB 1: VTAB 23: PRINT "PULS
     E B,C,D,E,F,P,S,T,O...";
510  GET R$
515  HTAB 27: VTAB 23: PRINT " ";

520  IF R$ <  > "B" THEN  GOTO 92
     0
550  GOSUB 8100
560  GOSUB 8200
570  PRINT "FRECUENCIA(" CHR$ (L +
     CA)")= " INT (1000 * C(L) +
     .5) / 10
```

```
575  IF C(L) = 0 THEN  GOTO 910
580  LET B = 1
590  FOR I = 1 TO 26
600  IF  ABS (E(I) - C(L)) > B THEN
      GOTO 630
610 B =  ABS (E(I) - C(L))
620 P = I
630  NEXT I
640  PRINT "SUGERENCIA: "; CHR$ (
     P + CA)
650  FOR X = 1 TO 26:N(X) = 0: NEXT

660  FOR I = 2 TO LT
670  IF T$(I) <  > L$ THEN  GOTO
     800
680 J = 0
683 J = J + 1
687  IF I - J < 1 THEN  GOTO 800
690  IF P$(I - J) = "*" THEN  GOTO
     800
695  IF P$(I - J) = " " THEN  GOTO
     683
700 T =  ASC (P$(I - J)) - CA
710  FOR J = 1 TO 26
720  LET N(J) = N(J) + T(T,J)
730  NEXT J
800  NEXT I
810  FOR I = 2 TO (19 - BL) * 2
820 B = 0
830  FOR J = 1 TO 26
840  IF N(J) <  = B THEN  GOTO 87
     0
850 B = N(J)
860 P = J
870  NEXT J
880  IF B = 0 THEN  GOTO 910
885  HTAB 15: VTAB 3
890  PRINT "TRANSICION: "; CHR$ (
     P + CA);": ";N(P)
895 N(P) = 0
900  NEXT I
910  GOTO 500
920  IF R$ <  > "C" THEN  GOTO 95
     0
930  REM  COPY
940  GOTO 500
950  IF R$ <  > "D" THEN  GOTO 99
     0
960  GOSUB 8200
965  IF A$(L) <  > "*" THEN B$( ASC
     (A$(L)) - CA) = "*"
970 A$(L) = "*"
980  GOTO 320
990  IF R$ <  > "E" THEN  GOTO 10
     40
1000  GOSUB 8100
1010  GOSUB 8200
1020  PRINT L$;": "; INT (1000 *
     E(L) + .5) / 10
1030  GOTO 500
1040  IF R$ <  > "F" THEN  GOTO 1
     090
1050  GOSUB 8100
1060  GOSUB 8200
1070  PRINT L$;": "; INT (1000 *
     C(L) + .5) / 10
1080  GOTO 500
1090  IF R$ = "N" THEN  GOTO 500
1100  IF R$ <  > "P" THEN  GOTO 1
     200
1110  GOSUB 8100
1111  HTAB 1: VTAB 1
1120  INPUT "LETRAS ?";L$
1130  IF L$ = "0" THEN  GOTO 9999

1140  IF  LEN (L$) <  > 2 THEN  GOTO
     1120
1150 L1 =  ASC ( LEFT$ (L$,1)) -
     CA
1160 L2 =  ASC ( RIGHT$ (L$,1)) -
     CA
1170  IF L1 < 1 OR L1 > 26 OR L2 <
     1 OR L2 > 26 THEN  GOTO 1120

1180  PRINT L$;": ";T(L1,L2)
1190  GOTO 500
1200  IF R$ <  > "S" THEN  GOTO 1
     240
1210  HOME : VTAB 4: PRINT "SOLUC
     ION:"
1221  FOR X = 1 TO LT: PRINT P$(X
     );: NEXT : PRINT
1230  GOTO 9999
1240  IF R$ <  > "T" THEN  GOTO 1
     340
1250  GOSUB 8200
1260 LL = L
1270 Q$ = L$
1280  HTAB 12: VTAB 1: GOSUB 8205

1300  IF B$(L) <  > "*" THEN  GOTO
     1280
1310  IF A$(LL) <  > "*" THEN B$(
      ASC (A$(LL)) - CA) = "*"
1320 A$(LL) = L$
1325 B$(L) = Q$
1330  GOTO 320
1340  IF R$ = "0" THEN  GOTO 9999

1350  HTAB 27: VTAB 23: PRINT "?"
     ; CHR$ (7)
1370  GOTO 500
8000  HTAB 1: VTAB 24
8005  PRINT "PULSE CUALQUIER TECL
     A";
8010  GET R$
8030  IF R$ = "0" THEN  GOTO 9999

8040  HTAB 1: VTAB 24
8050  PRINT "
      "
8090  RETURN
8100  FOR I = BL TO 21
8110  HTAB 1 + I: VTAB 1: PRINT "
      "
8120  NEXT I
```

```
8130  HTAB BL + 1: VTAB 1
8140  RETURN
8200  HTAB 1: VTAB 1
8201  PRINT "
                    "
8202  HTAB 1: VTAB 1
8205  INPUT "LETRA?";L$
8210  IF  LEFT$ (L$,1) = "0" THEN
      GOTO 9999
8220  IF  LEN (L$) <  > 1 THEN  GOTO
      8200
8230 L =  ASC (L$) - CA
8240  IF L < 1 OR L > 26 THEN  GOTO
      8200
8250  RETURN
8300 T$ = "": FOR X = 1 TO LT:T$ =
      T$ + T$(X): NEXT : RETURN
9999  REM  FIN
```

ZIG-ZAG

```
10  REM    *** ZIG ZAG ***
12  REM    ***************
15  HOME
20  PRINT : PRINT  TAB( 4);"PROGR
     AMA DE CIFRADO 'ZIG ZAG'"
25  PRINT  TAB( 4);"-------------
     ----------------"
30  VTAB 7: HTAB 4: INPUT "MODO:
     ";M$
37  IF M$ = "0" THEN  GOTO 9999
40  PRINT : HTAB 4: INPUT "CLAVE:
     ";M
50  IF M$ <  > "C" AND M$ <  > "D
     " THEN  GOTO 30
60  GOTO 130
130  IF M < 3 THEN  GOTO 30
140  POKE 34,4
145  HOME
150  VTAB 6: HTAB 6: PRINT "MODO
     : ";M$;
160  PRINT "       CLAVE : ";M
165  REM   **** ACEPTA TEXTO Y
        Y QUITA ESPACIOS ****
170  VTAB 11: INPUT "TEXTO :";T$
172  FOR I = 1 TO  LEN (T$)
173 T1$ =  MID$ (T$,I,1)
174  IF T1$ = " " THEN  GOTO 176
175 T2$ = T2$ + T1$
176  NEXT I
178 T$ = T2$
180 LT =  LEN (T$)
185  DIM C$(LT)
190  IF LT > 0 THEN  GOTO 220
200  PRINT : PRINT "?"
210  GOTO 170
220  PRINT : PRINT : PRINT "-----
     ----------------------------
     ------"
232  IF M$ = "C" THEN  PRINT : PRINT
      TAB( 13);"TEXTO CIFRADO": PRINT
      TAB( 13);"-------------"
240 S = 2 * (M - 1)
250  IF M$ = "D" THEN  GOTO 390
260  FOR I = 1 TO LT STEP S
270  PRINT MID$ (T$,I,1);
275  NEXT I
280  FOR I = 1 TO M - 2
290  FOR J = 1 TO LT STEP S
300  IF J + 1 <  = LT THEN  PRINT
      MID$ (T$,J + I,1);
310  IF J + S - I <  = LT THEN  PRINT
      MID$ (T$,J + S - I,1);
330  NEXT J
340  NEXT I
350  FOR I = M TO LT STEP S
360  PRINT  MID$ (T$,I,1);
370  NEXT I
379  PRINT : PRINT : PRINT "-----
     ----------------------------
     ------"
380  GOTO 9999
390  REM  **** MODO DESCIFRADO **
     **
400 L = 0
410  FOR I = 1 TO LT STEP S
420 L = L + 1
430 C$(I) =  MID$ (T$,L,1)
440  NEXT I
450  FOR I = 1 TO M - 2
460  FOR J = 1 TO LT STEP S
470  IF J + I > LT THEN  GOTO 500

480 L = L + 1
490 C$(I + J) =  MID$ (T$,L,1)
500  IF J + S - I > LT THEN  GOTO
     540
510 L = L + 1
520 C$(J + S - I) =  MID$ (T$,L,1
     )
540  NEXT J
550  NEXT I
560  FOR I = M TO LT STEP S
570 L = L + 1
580 C$(I) =  MID$ (T$,L,1)
590  NEXT I
600  FOR I = 1 TO LT
601  PRINT C$(I);
605  NEXT I
610  VTAB 22: HTAB 2: PRINT "PULS
     A 'S' PARA SEGUIR, 'N' PARA
     ACABAR"
620  GET R$
630  IF R$ = "" THEN  GOTO 620
640  IF R$ = "S" THEN  GOTO 680
```

```
650  IF R$ = "N" THEN  GOTO 9999
660  GOTO 620
680 M = M + 1
685  HTAB 28: VTAB 6
690  PRINT M
695  VTAB 12
700  GOTO 220
9999  POKE 34,0: END : REM  FIN
```

COLUMNAS COMPLETAS

```
10  REM  **** COLUMNAS ****
         **** COMPLETAS ***
15  HOME
20  PRINT : PRINT "PROGRAMA DE CI
     FRADO 'COLUMNAS COMPLETAS'";
21  PRINT "----------------------
     ------------------"
30  VTAB 5: INPUT "MODO : ";M$
40  PRINT : INPUT "CLAVE : ";C$
50  IF  LEFT$ (M$,1) = "O" THEN  GOTO
     9999
55  IF  LEFT$ (M$,1) <  > "C" AND
      LEFT$ (M$,1) <  > "D" THEN
      GOTO 30
60  IF  LEN (C$) < 2 THEN  GOTO 3
     0
80  POKE 34,9
110 LC =  LEN (C$)
120  DIM K(LC),CM$(LC)
121  FOR M = 1 TO LC
122 CM$(M) =  MID$ (C$,M,1)
123  NEXT M
130  FOR I = 1 TO LC
140 B$ = "^"
160  FOR J = 1 TO LC
170  IF CM$(J) >  = B$ THEN  GOTO
     200
180 B$ = CM$(J)
190 P = J
200  NEXT J
210 CM$(P) = "^"
216 K(I) = P
217  NEXT I
219  POKE 34,4
220  HOME
221  VTAB 5: PRINT "MODO : ";M$
230  PRINT : PRINT "CLAVE : ";C$
231  POKE 34,10
232  PRINT : PRINT "-------------
     ----------------------------"
240  VTAB 12: INPUT "TEXTO : ";T$
250  FOR I = 1 TO  LEN (T$)
260  IF I >  =  LEN (T$) THEN  GOTO
     300
270  IF  MID$ (T$,I,1) <  > " " THEN
      GOTO 300
278  IF I = 1 THEN T$ =  RIGHT$ (
     T$, LEN (T$) - 1): GOTO 290
280 T$ =  LEFT$ (T$,I - 1) +  RIGHT$
     (T$, LEN (T$) - I)
290  GOTO 260
300  NEXT I
310  IF  LEFT$ (T$,1) = "O" THEN
      GOTO 9999
320  IF  LEN (T$) > 0 THEN  GOTO
     350
330  REM  *** REINTRODUCE TEXTO *
     **
340  GOTO 230
350 LT =  LEN (T$)
360  IF (LT / LC) =  INT (LT / LC
     ) THEN  GOTO 390
370 T$ = T$ +  CHR$ (65 +  INT (2
     6 *  RND (1)))
380  GOTO 350
390  PRINT : PRINT "TEXTO : ";T$
400  PRINT
401  DIM TM$(LT)
402  FOR M = 1 TO LT
403 TM$(M) =  MID$ (T$,M,1)
404  NEXT M
410  IF  LEFT$ (M$,1) = "D" THEN
      GOTO 480
420 H = 0
425  FOR I = 1 TO LC
430  FOR J = K(I) TO LT STEP LC
435 H = H + 1
440  PRINT TM$(J);
445  IF H / 5 =  INT (H / 5) THEN
      PRINT " ";
450  NEXT J
460  NEXT I
470  GOTO 9999
480  DIM CB$(LT)
481  FOR H = 1 TO LT
482  IF H > LC THEN  GOTO 489
483 CB$(H) = CM$(H)
489  NEXT H
490 L = 0
500  FOR I = 1 TO LC
510  FOR J = K(I) TO LT STEP LC
520 L = L + 1
521  IF L > LT THEN  GOTO 540
530 CB$(J) = TM$(L)
540  NEXT J
550  NEXT I
560  FOR H = 1 TO LT
570  PRINT CB$(H);
575  IF H / 5 =  INT (H / 5) THEN
      PRINT " ";
580  NEXT H
9999  POKE 34,0: END : REM  FIN
```

TRANSPOSICION DE ITINERARIO

```
10  REM   TRANSPOSICION DE ITINER
    ARIO
15 D$ =  CHR$ (4)
20  DIM L$(50),C$(25)
22  PRINT "LEO DATOS DE DISCO";: GET
    R$
24  IF R$ = "S" GOTO 1600
30  FOR R = 1 TO 32
40  READ L$(R)
50  NEXT R
60  DATA   "AFKPUBGLQVCHMRWDINSXE
    JOTY"
70  DATA  "UPKFAVQLGBWRMHCXSNIDYT
    OJE"
80  DATA  "EJOTYDINSXCHMRWBGLQVAF
    KPU"
90  DATA  "YTOJEXSNIDWRMHCVQLGBUP
    KFA"
100  DATA  "ABCDEFGHIJKLMNOPQRSTU
    VWXY"
110  DATA  "UVWXYPQRSTKLMNOFGHIJA
    BCDE"
120  DATA  "EDCBAJIHGFONMLKTSRQPY
    XWVU"
130  DATA   "YXWVUTSRQPONMLKJIHGF
    EDCBA"
140  DATA  "OSVXYJNRUWFIMQTCEHLPA
    BDGK"
150  DATA  "OJFCASNIEBVRMHDXUQLGY
    WTPK"
160  DATA  "ACFJOBEINSDHMRVGLQUXK
    PTWY"
170  DATA  "YXVSOWURNJTQMIFPLHECK
    GDBA"
180  DATA  "KPTWYGLQUXDHMRVBEINSA
    CFJO"
190  DATA  "KGDBAPLHECTQMIFWURNJY
    XVSO"
200  DATA  "ABDGKCEHLPFIMQTJNRUWO
    SVXY"
210  DATA  "YWTPKXUQLGVRMHDSNIEBO
    JFCA"
220  DATA  "EFOPYDGNQXCHMRWBILSVA
    JKTU"
230  DATA  "YPOFEXQNGDWRMHCVSLIBU
    TKJA"
240  DATA  "AJKTUBILSVCHMRWDGNQXE
    FOPY"
250  DATA  "UTKJAVSLIBWRMHCXQNGDY
    POFE"
260  DATA  "ABCDEJIHGFKLMNOTSRQPU
    VWXY"
270  DATA  "UVWXYTSRQPKLMNOJIHGFA
    BCDE"
280  DATA  "EDCBAFGHIJONMLKPQRSTY
    XWVU"
290  DATA  "YXWVUPQRSTONMLKFGHIJE
    DCBA"
300  DATA  "ABFGOCEHNPDIMQVJLRUWK
    STXY"
310  DATA   "YXTSKWURLJVQMIDPNHEC
    OGFBA"
320  DATA  "ACDJKBEILSFHMRTGNQUXO
    PVWY"
330  DATA   "YWVPOXUQNGTRMHFSLIEB
    KJDCA"
340  DATA  "OPVWYGNQUXFHMRTBEILSA
    CDJK"
350  DATA  "KJDCASLIEBTRMHFXUQNGY
    WVPO"
360  DATA  "KSTXYJLRUWDIMQVCEHNPA
    BFGO"
370  DATA  "OGFBAPNHECVQMIDWURLJY
    XTSK"
377 CA =  ASC ("A") - 1
380  HOME
390  PRINT : PRINT "TRANSPOSICION
     DE ITINERARIO"
391  PRINT "----------------------
     ------"
400  VTAB 5: INPUT "MODO: ";M$
420  IF M$ = "O" THEN  GOTO 9999
430  IF M$ = "L" THEN  GOTO 1010
440  IF M$ = "S" THEN  GOTO 1510
450  IF M$ < "C" OR M$ > "D" THEN
     GOTO 400
460  PRINT : INPUT "NUMERO CLAVE:
     ";NC$
470  IF  LEN (NC$) < 1 THEN  GOTO
     400
471 F = 0
480  FOR I = 1 TO  LEN (NC$)
490 N1C$ =  MID$ (NC$,I,1)
495  IF N1C$ < "0" OR N1C$ > "9" THEN
     F = 1
500  NEXT I
505  IF F = 1 THEN  GOTO 400
510 K =  VAL (NC$)
520  IF K < 1 OR K  = R THEN  GOTO
     400
530  PRINT : PRINT "ITINERARIO :
     "
535  VTAB 9
540  FOR Y = 0 TO 4
550  HTAB 14: PRINT  MID$ (L$(K),
     Y * 5 + 1,5)
560  NEXT Y
565  PRINT
570  INPUT "TEXTO: ";T$
590  FOR I = 1 TO  LEN (T$)
600  IF I >  LEN (T$) THEN  GOTO
     670
```

```
610 T1$ =  MID$ (T$,I,1)
615  IF T1$ <  > " " THEN  GOTO 6
     70
620 R$ = ""
630  IF I > 1 THEN R$ =  LEFT$ (T
     $,I - 1)
640  IF I <  LEN (T$) THEN R$ = R
     $ +  RIGHT$ (T$, LEN (T$) -
     I)
650 T$ = R$
660  GOTO 600
670  NEXT I
680  IF  LEFT$ (T$,1) = "O" THEN
      GOTO 9999
690 LT =  LEN (T$)
700  IF LT > 0 THEN  GOTO 730
710  GOTO 570
730  IF LT / 25 =  INT (LT / 25) THEN
      GOTO 770
740 T$ = T$ +  CHR$ (65 +  INT (2
     5 *  RND (1)))
750 LT = LT + 1
760  GOTO 730
770  PRINT : PRINT "TEXTO: ";T$
780  PRINT
790  IF M$ = "D" THEN  GOTO 920
810  FOR I = 1 TO 25
820  FOR J = 1 TO 25
830  IF  MID$ (L$(K),J,1) =  CHR$
     (CA + I) THEN C$(J) =  MID$
     (T$,I,1)
840  NEXT J
850  NEXT I
860  FOR S = 1 TO 25
861  PRINT C$(S);
862  NEXT S
863  PRINT
870  IF LT = 25 THEN  PRINT : PRINT
     "PULSA UNA TECLA. ";: GET A$
     : GOTO 380
880 T$ =  RIGHT$ (T$, LEN (T$) -
     25)
890 LT = LT - 25
900  GOTO 810
920  FOR I = 1 TO 25
930  FOR J = 1 TO 25
940  IF  MID$ (L$(K),J,1) =  CHR$
     (CA + I) THEN C$(I) =  MID$
     (T$,J,1)
950  NEXT J
960  NEXT I
970  FOR I = 1 TO 25
971  PRINT C$(I);
972  NEXT I
973  PRINT
975  IF LT = 25 THEN  PRINT : PRINT
     "PULSA UNA TECLA. ";: GET A$
     : GOTO 380
980 T$ =  RIGHT$ (T$, LEN (T$) -
     25)
990 LT = LT - 25
1000  GOTO 920
1010  IF R <  = 50 THEN  GOTO 107
     0
1020  PRINT : PRINT "LIBRERIA COM
     PLETA."
1030  PRINT  CHR$ (7)
1040  GOTO 400
1070  PRINT : PRINT "RUTA NUMERO
     ";R;"                    "
1080  FOR X = 0 TO 4
1090  VTAB X + 14: INPUT "";M$(X)

1100  IF  LEN (M$(X)) <  > 5 GOTO
     1090
1110  FOR Y = 1 TO 5
1120  IF ( MID$ (M$(X),Y,1) < "A"
     ) OR ( MID$ (M$(X),Y,1) > "Z
     ") GOTO 1090
1130  NEXT Y
1140  NEXT X
1150 C$ = ""
1160  FOR X = 0 TO 4
1170 C$ = C$ + M$(X)
1180  NEXT X
1190  FOR X = 2 TO 25
1200  FOR Y = 1 TO X - 1
1210  IF  MID$ (C$,X,1) =  MID$ (
     C$,Y,1) THEN  GOTO 1080
1220  NEXT Y
1230  NEXT X
1240 L$(R) = C$
1495 R = R + 1
1500  GOTO 380
1510  HOME
1520  VTAB 10: INPUT "CON QUE NOM
     BRE QUIERES SALVARLO? ";N$
1530  PRINT D$;"OPEN";N$
1540  PRINT D$;"WRITE";N$
1550  FOR I = 1 TO 50
1560  PRINT L$(I)
1570  NEXT I
1575  PRINT R
1580  PRINT D$;"CLOSE";N$
1590  GOTO 380
1600  HOME
1610  PRINT "NOMBRE DEL FICHERO "
     ;
1620  INPUT N$
1630  PRINT D$;"OPEN";N$
1640  PRINT D$;"READ";N$
1650  FOR I = 1 TO 50
1660  INPUT L$(I)
1670  NEXT I
1675  INPUT R
1680  PRINT D$;"CLOSE";N$
1690  GOTO 377
9999  END
```

REJILLA DE CARDANO

```
10  REM  REJILLA DE CARDANO
15  HOME
20  PRINT "PROGRAMA DE CIFRADO RE
     JILLA DE CARDANO"
30  HTAB 2: VTAB 2: INPUT "MODO:
     ";M$
50  IF M$ = "O" THEN  GOTO 9999
60  IF M$ = "C" OR M$ = "D" THEN
      GOTO 90
70  VTAB 2: HTAB 1: PRINT "?"
80  GOTO 30
90  VTAB 2: HTAB 1: PRINT "MODO :
      ";M$
93  DIM G(6,6)
97 NH = 0
190  FOR Q = 1 TO 4
200 SX = 24
210  IF Q = 2 OR Q = 3 THEN SX =
     28
220 SY = 3
230  IF Q > 2 THEN SY = 7
240  VTAB SY: HTAB SX: PRINT "123
     ";: VTAB SY + 1: HTAB SX: PRINT
     "456";: VTAB SY + 2: HTAB SX
     : PRINT "789"
250  VTAB 4: HTAB 1: PRINT "CUADR
     ANTE ";Q;" AGUJERO?"
260  VTAB 4: HTAB 21
270  GET R$
280  IF R$ = "" THEN  GOTO 270
290  IF R$ = "O" THEN  GOTO 9999
300  IF R$ = "N" THEN  GOTO 620
310  IF R$ >  = "1" AND R$ <  = "
     9" THEN  GOTO 350
320  VTAB 4: HTAB 18: PRINT "?"
330  PRINT  CHR$ (7)
340  GOTO 260
350 V =  VAL (R$)
360  PRINT V
370 GY =  INT ((V - 1) / 3) + 1
380 GX = V - 3 * (GY - 1)
390  IF Q = 2 OR Q = 3 THEN GX =
     GX + 3
400  IF Q > 2 THEN GY = GY + 3
410  IF G(GY,GX) = 1 THEN  GOTO 3
     30
420  FOR Y = 1 TO 6
430  FOR X = 1 TO 6
440  IF G(Y,X) = 0 THEN  GOTO 530

450 YY = Y
460 XX = X
470  FOR R = 1 TO Q - 1
480 I = YY
490 YY = XX
500 XX = 7 - I
510  IF YY = GY AND XX = GX THEN
      GOTO 330
520  NEXT R
530  NEXT X
540  NEXT Y
550 G(GY,GX) = 1
560  IF GX > 3 THEN GX = GX + 1
570  IF GY > 3 THEN GY = GY + 1
580  VTAB 2 + GY: HTAB 23 + GX: PRINT
     " "
590 NH = NH + 1
600  IF NH < 9 THEN  GOTO 260
610 Q = 4
620  IF Q = 4 AND NH < 9 THEN  GOTO
     320
680  NEXT Q
690  VTAB 4: HTAB 1: PRINT  TAB(
     19)
700  VTAB 12: HTAB 2: PRINT "TEXT
     O : ";
710  INPUT "";T$
720  FOR I = 1 TO  LEN (T$)
730  IF I >  LEN (T$) THEN  GOTO
     800
740  IF  MID$ (T$,I,1) <  > " " THEN
      GOTO 800
750 R$ = ""
760  IF I > 1 THEN R$ =  LEFT$ (T
     $,I - 1)
770  IF I <  LEN (T$) THEN R$ = R
     $ +  RIGHT$ (T$, LEN (T$) -
     I)
780 T$ = R$
790  GOTO 730
800  NEXT I
810  IF T$ = "O" THEN  GOTO 9999
820 LT =  LEN (T$)
830  IF LT / 36 =  INT (LT / 36) THEN
      GOTO 870
840 T$ = T$ + "Z"
850 LT = LT + 1
860  GOTO 830
870  VTAB 12: HTAB 1: PRINT "TEXT
     O : ";T$
880  PRINT
890  DIM C$(6,6)
895 RF = 1
900  IF M$ = "D" THEN  GOTO 1110
910 CN = 0
920  FOR Q = 1 TO 4
930  FOR Y = 1 TO 6
940  FOR X = 1 TO 6
950  IF G(Y,X) = 0 THEN  GOTO 980

960 CN = CN + 1
970 C$(Y,X) =  MID$ (T$,CN,1)
980  NEXT X
990  NEXT Y
1000  GOSUB 2000
1010  NEXT Q
1020  FOR Y = 1 TO 6
1030  FOR X = 1 TO 6
```

```
1040  PRINT C$(Y,X);
1050  NEXT X
1060  NEXT Y
1070  IF LT = 36 THEN  GOTO 9999
1080 T$ =  RIGHT$ (T$, LEN (T$) -
     36)
1090 LT = LT - 36
1100  GOTO 910
1110 CN = 0
1120  FOR Y = 1 TO 6
1130  FOR X = 1 TO 6
1140 CN = CN + 1
1150 C$(Y,X) =  MID$ (T$,CN,1)
1160  NEXT X
1170  NEXT Y
1180  FOR Q = 1 TO 4
1190  FOR Y = 1 TO 6
1200  FOR X = 1 TO 6
1210  IF G(Y,X) > 0 THEN  PRINT C
     $(Y,X);
1220  NEXT X
1230  NEXT Y
1240  GOSUB 2000
1250  NEXT Q
1260  IF LT = 36 THEN  GOTO 9999
1270 T$ =  RIGHT$ (T$, LEN (T$) -
     36)
1280 LT = LT - 36
1290  GOTO 1110
2000  FOR Y = 1 TO 6
2010  FOR X = 1 TO 6
2020  IF G(Y,X) <  > RF THEN  GOTO
     2070
2030 G(Y,X) = 0
2040 YY = X
2050 XX = 7 - Y
2060 G(YY,XX) = 3 - RF
2070  NEXT X
2080  NEXT Y
2090 RF = 3 - RF
2100  RETURN
9999  REM  FIN
```

ANALISIS POR COLUMNAS COMPLETAS

```
10  REM  ANALISIS DE COLUMNAS COM
     PLETAS
20  DIM E(26),T(26,26)
25 NR = 30:NC = 15: DIM C$(NR,NC)
    ,P$(NR,NC),B(NC),F(NC)
30 D$ =  CHR$ (4)
40  HOME : PRINT "INSERTE EL DISC
    O DE DATOS                Y P
    ULSE UNA TECLA.";: GET A$
45  PRINT
46  PRINT D$;"OPEN TRANSICION"
50  PRINT D$;"READ TRANSICION"
55  FOR F = 1 TO 26: FOR C = 1 TO
     26: INPUT T(F,C): NEXT : NEXT
60  PRINT D$;"CLOSE TRANSICION"
70  HOME
80  PRINT "ANALISIS COMPLETO DE C
    OLUMNAS"
90  HTAB 3: VTAB 3: PRINT "TEXTO:
     ";
100  INPUT T$
110  FOR I = 1 TO  LEN (T$)
120  IF I >  LEN (T$) THEN  GOTO
     190
130  IF  MID$ (T$,I,1) <  > " " THEN
      GOTO 190
140 R$ = ""
150  IF I > 1 THEN R$ =  LEFT$ (T
     $,I - 1)
160  IF I <  LEN (T$) THEN R$ = R
     $ +  RIGHT$ (T$, LEN (T$) -
     I)
170 T$ = R$
180  GOTO 120
190  NEXT I
200  IF T$ = "0" THEN  GOTO 9999
210 LT =  LEN (T$)
220  IF LT > 0 THEN  GOTO 250
230  HTAB 1: VTAB 3: PRINT "?"
240  GOTO 90
250 NF = 0
260  FOR I = 2 TO  INT (LT / 2)
270  IF LT / I =  INT (LT / I) THEN
     NF = NF + 1
280  NEXT I
290  IF NF = 0 THEN  GOTO 230
300  DIM C(NF)
310  DIM R(NF)
320 NF = 0
330  FOR I = 2 TO  INT (LT / 2)
340  IF LT / I >  INT (LT / I) THEN
      GOTO 380
350 NF = NF + 1
360 C(NF) = I
370 R(NF) = LT / I
380  NEXT I
385 CA =  ASC ("A") - 1
390  HTAB 1: PRINT "TEXTO: ";T$
400  PRINT
410  PRINT "HAY ";NF;" METODOS DE
```

```
      FACTORIZACION"
420   PRINT
430   FOR I = 1 TO NF
440   INVERSE : PRINT I;: NORMAL :
       PRINT ": ";R(I);" FILAS ";C
      (I);" COLUMNAS."
445   NEXT I
450   PRINT
460   PRINT "DISTRIBUCION DE VOCAL
      ES (S/N/O).?";
490   GET R$
500   IF R$ = "O" THEN  GOTO 9999
510   IF R$ = "N" THEN  GOTO 650
515   HOME
520   FOR I = 1 TO NF
530   INVERSE : PRINT I;: NORMAL :
       PRINT ": ";R(I);" X ";C(I);
      ": ";
540   FOR J = 1 TO R(I)
550 NV = 0
560   FOR K = 1 TO C(I)
570 R$ =  MID$ (T$,(K - 1) * R(I)
       + J,1)
580   IF R$ = "A" OR R$ = "E" OR R
      $ = "I" OR R$ = "O" OR R$ =
      "U" THEN NV = NV + 1
590   NEXT K
600   PRINT  INT (NV / C(I) * 100)
      ;: PRINT "%";
610   NEXT J
620   PRINT
630   PRINT
640   NEXT I
650   PRINT
660   INPUT "NUMERO DEL BLOQUE DE
      DIMENSIONES ";R$
665 BD =  VAL (R$)
667   IF BD = 0 THEN  GOTO 9999
670   IF BD < 1 OR (BD > NF) OR BD
       >  INT (BD) THEN  GOTO 660
680 NC = C(BD)
690 NR = R(BD)
691   REM
692   FOR I = 1 TO NR
693   FOR J = 1 TO NC
694 C$(I,J) =  MID$ (T$,(J - 1) *
      NR + I,1)
695   NEXT J
696   NEXT I
697   FOR I = 1 TO NC:F(I) = 0:B(I
      ) = 0: NEXT
700   HOME
710   FOR I = 1 TO NC
720   HTAB I: VTAB 1: PRINT  INT (
      I / 10);: HTAB 16 + I: VTAB
      1: PRINT  INT (I / 10)
730   HTAB I: VTAB 2: PRINT I - 10
       *  INT (I / 10);: HTAB 16 +
      I: VTAB 2: PRINT I - 10 *  INT
      (I / 10)
740   HTAB I: VTAB 3: PRINT "-": HTAB
      16 + I: VTAB 3: PRINT "-"
750   NEXT I
760   FOR I = 1 TO NR
770   FOR J = 1 TO NC: PRINT C$(I,
      J);: NEXT J: PRINT
780   NEXT I
790   GOSUB 8000
810 F(CN) = 1
820 B(1) = CN
830   GOSUB 8100
840   HTAB 1: VTAB 20: PRINT : HTAB
      1: VTAB 20: PRINT "PULSA W,D
      ,I,L,R,P,B,S,O...";
850   GET R$
860   HTAB 1: VTAB 20: PRINT
867   IF R$ = "B" THEN  HOME : GOTO
      390
890   IF R$ = "O" THEN  GOTO 9999
900   IF R$ <  > "L" AND R$ <  > "
      R" THEN  GOTO 1160
910   GOSUB 8050
915   IF B(PC) = 0 THEN  GOTO 910
920 C = B(PC)
930   POKE 34,NR + 5: HOME : POKE
      34,1
1010  FOR I = 1 TO NC
1020  IF I = C THEN  GOTO 1140
1030  PRINT I;
1050  PRINT ": ";
1060 P = 0
1070  FOR J = 1 TO NR
1080 CP =  ASC (C$(J,C)) - CA
1090 TC =  ASC (C$(J,I)) - CA
1100  IF R$ = "L" THEN P = P + T(
      TC,CP)
1110  IF R$ = "R" THEN P = P + T(
      CP,TC)
1120  NEXT J
1130  PRINT P;
1135  PRINT
1140  NEXT I
1151  PRINT "PULSE UNA TECLA.";: GET
      R$
1152  POKE 34,NR + 5: HOME : POKE
      34,1
1153  GOTO 840
1160  IF R$ <  > "D" THEN  GOTO 1
      250
1170  GOSUB 8050
1175  IF B(PC) > 0 THEN F(B(PC)) =
      0:B(PC) = 0
1180  FOR I = PC TO NC - 1
1190 B(I) = B(I + 1)
1200  IF B(I) > 0 THEN F(B(I)) =
      I
1210  NEXT I
1220 B(NC) = 0
1230  GOSUB 8100
1240  GOTO 840
1250  IF R$ <  > "I" THEN  GOTO 1
      301
1255  GOSUB 8050
1257 F(B(NC)) = 0
1259  IF PC >  = NC THEN  GOTO 12
      90
```

```
1260  FOR I = NC TO PC + 1 STEP  -
      1
1270 B(I) = B(I - 1)
1280  IF B(I) > 0 THEN F(B(I)) =
      I
1285  NEXT I
1292 B(PC) = 0
1294  GOSUB 8100
1300  GOTO 840
1301  IF R$ <  > "W" THEN  GOTO 1
      310
1302  GOSUB 8050
1303  GOSUB 8000
1304  IF B(PC) > 0 THEN F(B(PC)) =
      0
1305 F(CN) = PC
1306 B(PC) = CN
1307  GOSUB 8100
1308  GOTO 840
1310  IF R$ <  > "P" THEN  GOTO 1
      319
1311  HTAB 1: VTAB 22: PRINT "
                          ": VTAB 2
      2: INPUT "LETRAS: ";R$
1312  IF  LEN (R$) <  > 2 THEN  GOTO
      1311
1313 L1 =  ASC ( LEFT$ (R$,1)) -
      CA
1314 L2 =  ASC ( RIGHT$ (R$,1)) -
      CA
1315  IF L1 < 1 OR L1 > 26 OR L2 <
      1 OR L2 > 26 THEN  GOTO 1311

1316  HTAB 14: VTAB 22: PRINT "FR
      EC=";T(L1,L2)
1318  GOTO 840
1319  IF R$ = "S" THEN  GOTO 1350

1320  HTAB 1: VTAB 21: PRINT "?"
1330  PRINT  CHR$ (7)
1340  GOTO 840
1350  HOME : VTAB 4: PRINT "SOLUC
      ION:"
1360  FOR J = 1 TO NR
1365  FOR I = 1 TO NC
1370  PRINT C$(J,B(I));
1380  NEXT : NEXT
1390  GOTO 9999
4000 T$ = "LRBLR SNELO ASILR TSLU
      E AEAAB AENEJ LVARI IIEAI LO
      RAE IELQT"
5000  PRINT "♦OPENTEXTO"
5001  PRINT "♦WRITE TEXTO"
5003  PRINT T$
5005  PRINT "♦CLOSE TEXTO"
5006  END
8000  HTAB 1: VTAB 23: INPUT "NUM
      ERO DE COLUMNA A PONER: ";CN
8010 CN =  INT (CN)
8020  IF CN = 0 THEN  GOTO 9999
8030  IF CN < 1 OR CN > NC THEN  GOTO
      8000
8035  IF F(CN) > 0 THEN  GOTO 800
      0
8040  RETURN
8050  HTAB 1: VTAB 22: PRINT "
                          "
8051  HTAB 1: VTAB 22: INPUT "POS
      ICION: ";PC
8060 PC =  INT (PC)
8070  IF PC = 0 THEN  GOTO 9999
8080  IF PC < 1 OR PC > NC THEN  GOTO
      8050
8090  RETURN
8100  FOR I = 1 TO NR: FOR J = 1 TO
      NC:P$(I,J) = " ": NEXT J: NEXT
      I
8110  FOR I = 1 TO NC
8115  HTAB I: VTAB 3: PRINT "-"
8120 C = F(I)
8130  IF C = 0 THEN  GOTO 8170
8135  HTAB I: VTAB 3: INVERSE : PRINT
      "-": NORMAL
8140  FOR J = 1 TO NR
8150  LET P$(J,C) = C$(J,I)
8160  NEXT J
8170  NEXT I
8180  FOR I = 1 TO NR
8190  HTAB 17: VTAB 3 + I: FOR J =
      1 TO NC: PRINT P$(I,J);: NEXT
      J: PRINT
8200  NEXT I
8210  RETURN
9000 D$ =  CHR$ (4)
9010  PRINT "INTRODUZCA EL DISCO
      DE DATOS Y PULSE   UNA TECLA
      : ";: GET N$
9020  PRINT D$;"OPEN FRECUENCIA"
9030  PRINT D$;"READ FRECUENCIA"
9040  FOR I = 1 TO 26
9050  INPUT E(I)
9060  NEXT I
9070  PRINT D$;"CLOSE FRECUENCIA"

9080  PRINT D$;"OPEN TRANSICION"
9090  PRINT D$;"READ TRANSICION"
9100  FOR X = 1 TO 26
9110  FOR Y = 1 TO 26
9120  INPUT T(X,Y)
9130  NEXT Y
9140  NEXT X
9150  PRINT D$;"CLOSE TRANSICION"
9160  RETURN
9999  REM  FIN
```

ANALISIS POR LA REJILLA DE CARDANO

```
10  REM  ANALISIS DE REJILLA DE C
    ARDANO
40  DIM E(26),T(26,26)
50  DIM G(6,6),A(6,6)
60  GOSUB 9000
70  HOME
80  PRINT "ANALISIS DE REJILLA DE
    CARDANO"
90  HTAB 3: VTAB 2: PRINT "TEXTO
    ";
91  PRINT "♦OPEN TEXTO"
92  PRINT "♦READ TEXTO"
100  INPUT T$
101  PRINT "♦CLOSE TEXTO"
110  IF T$ = "0" THEN  GOTO 9999
120  FOR I = 1 TO  LEN (T$)
130  IF I >  LEN (T$) THEN  GOTO
    200
140  IF  MID$ (T$,I,1) >  = "A" AND
     MID$ (T$,I,1) <  = "Z" GOTO
    200
150 R$ = ""
160  IF I > 1 THEN R$ =  LEFT$ (T
    $,I - 1)
170  IF I <  LEN (T$) THEN R$ = R
    $ +  RIGHT$ (T$, LEN (T$) -
    I)
180 T$ = R$
190  GOTO 130
200  NEXT I
210 LT =  LEN (T$)
220  IF LT = 0 THEN  GOTO 240
230  IF LT / 36 =  INT (LT / 36) THEN
     GOTO 260
235 T$ = T$ + "Z"
240 LT = LT + 1
250  GOTO 230
260  PRINT "TEXTO: ";T$
270 NB =  INT (LT / 36)
310 CA =  ASC ("A") - 1
370  HTAB 1: VTAB 21: PRINT "PULS
    E UNA TECLA  "
380  GET R$
390  IF R$ = "0" THEN  GOTO 9999
430  HOME
440  FOR I = 1 TO 6
450  FOR J = 1 TO 6
460 G(J,I) = 0
470 A(J,I) = 0
480  NEXT J
490  NEXT I
510  HTAB 14: VTAB 1: PRINT "1234
    56"
520  FOR I = 1 TO 6
530  HTAB 12: VTAB I + 2: PRINT I
540  NEXT I
541 NH = 0
545 R$ = ""
550  GOTO 700
560  HTAB 1: VTAB 22: PRINT "PULS
    AR D,H,L,R,P,T,N,O...";
570  GET R$
630  IF R$ <  > "D" THEN  GOTO 69
    0
640  GOSUB 8000
650 G(Y,X) = 0
660  HTAB 13 + X: VTAB 2 + Y: PRINT
    " "
670 NH = NH - 1
680  GOTO 560
690  IF R$ <  > "H" THEN  GOTO 74
    0
700  GOSUB 8000
710 G(Y,X) = 1
720  HTAB 13 + X: VTAB 2 + Y: INVERSE
    : PRINT " ": NORMAL
725 NH = NH + 1
730  GOTO 560
740  IF R$ <  > "L" AND R$ <  > "
    R" THEN  GOTO 1105
745  GOSUB 8200
750  GOSUB 8000
752  POKE 34,10
753 XX = X
757 YY = Y
760  IF R$ = "L" THEN  GOTO 830
770 X = X + 1
780  IF X <  = 6 THEN  GOTO 915
790 X = 1
800 Y = Y + 1
810  IF Y > 6 THEN  GOTO 1100
820  GOTO 880
830 X = X - 1
840  IF X >  = 1 THEN  GOTO 915
850 X = 6
860 Y = Y - 1
870  IF Y < 1 THEN  GOTO 1100
880  REM
915 P = 0
917  FOR I = 1 TO NB
920  FOR J = 1 TO 2
960  IF R$ = "R" THEN P = P + T( ASC
    ( MID$ (T$,(I - 1) * 36 + (Y
    Y - 1) * 6 + XX,1)) - CA, ASC
    ( MID$ (T$,(I - 1) * 36 + (Y
     - 1) * 6 + X,1)) - CA)
970 X = 7 - X
980 Y = 7 - Y
990 XX = 7 - XX
1000 YY = 7 - YY
1010 R$ =  CHR$ ( ASC ("R") +  ASC
    ("L") -  ASC (R$))
```

```
1020  NEXT J
1025  NEXT I
1030  INVERSE
1040  FOR I = 1 TO 4
1050  GOSUB 8100
1060  IF G(X,Y) = 1 THEN  NORMAL

1070  NEXT I
1080  PRINT X;",";Y;: NORMAL : PRINT
      ": ";P,
1090  GET A$: IF A$ <  > "F" GOTO
      760
1100  HOME : POKE 34,0: GOTO 560
1105  IF R$ = "N" THEN  GOTO 430
1110  IF R$ <  > "P" THEN  GOTO 1
      200
1120  GOSUB 8200
1130  INPUT "LETRAS : ";L$
1140  IF  LEN (L$) <  > 2 THEN  GOTO
      1130
1150 L1 =  ASC ( MID$ (L$,1,1)) -
      CA
1160 L2 =  ASC ( MID$ (L$,2,1)) -
      CA
1170  IF L1 < 1 OR L1 > 26 OR L2 <
      1 OR L2 > 26 THEN  GOTO 1130

1180  INVERSE : PRINT L$;: NORMAL
      : PRINT ": ";T(L1,L2)
1190  GOTO 560
1200  IF R$ <  > "T" THEN  GOTO 1
      460
1205  IF NH = 9 THEN  GOTO 1210
1207  PRINT "";
1208  GOTO 560
1210 RF = 1
1211  FOR Y = 1 TO 6
1212  FOR X = 1 TO 6
1213 A(Y,X) = G(Y,X)
1214  NEXT X
1215  NEXT Y
1219  FOR I = 1 TO 4
1220  GOSUB 8200
1225  FOR J = 1 TO NB
1230  FOR K = 1 TO 4
1240  FOR Y = 1 TO 6
1250  FOR X = 1 TO 6
1260  IF A(Y,X) <  > RF THEN  GOTO
      1270
1261  PRINT  MID$ (T$,(J - 1) * 3
      6 + (Y - 1) * 6 + X,1);
1262 A(Y,X) = 0
1263 A(X,7 - Y) = 3 - RF
1270  NEXT X
1280  NEXT Y
1290 RF = 3 - RF
1300  NEXT K
1310  NEXT J
1320  HTAB 1: VTAB 22: PRINT "PUL
      SAR N,R,S,O...";
1330  GET R$
1345  HTAB 1: VTAB 22: PRINT  TAB(
      39)
1380  IF R$ <  > "N" THEN  GOTO 1
      410
1381  FOR Y = 1 TO 6
1382  FOR X = 1 TO 6
1383  IF A(Y,X) <  > RF THEN  GOTO
      1386
1384 A(Y,X) = 0
1385 A(X,7 - Y) = 3 - RF
1386  NEXT X
1387  NEXT Y
1388 RF = 3 - RF
1390  NEXT I
1400  GOTO 1219
1410  IF R$ = "R" THEN  GOTO 560
1420  IF R$ = "F" OR R$ = "O" THEN
      GOTO 9999
1430  HTAB 1: VTAB 22: PRINT "?"
1440  PRINT "";
1450  GOTO 1320
1460  IF R$ = "O" THEN  GOTO 9999

1480  PRINT "";
1490  GOTO 560
4500  DIM A(6,6)
8000  VTAB 15: HTAB 2: INPUT "POS
      ICION: X,Y?";X,Y
8005  IF X = 0 OR Y = 0 THEN  GOTO
      9999
8010  IF (X < 1) OR (X > 6) OR (X
      >  INT (X)) OR (Y < 1) OR (
      Y > 6) OR (Y >  INT (Y)) THEN
       GOTO 8000
8020  IF R$ = "D" OR R$ = "L" OR
      R$ = "R" THEN  GOTO 8080
8030  FOR I = 1 TO 4
8040  GOSUB 8100
8050  IF G(Y,X) <  > 0 THEN  GOTO
      8090
8060  NEXT I
8070  RETURN
8080  IF G(Y,X) = 1 THEN  GOTO 80
      70
8090  PRINT "";
8095  GOTO 8000
8100 S = Y
8110 Y = 7 - X
8120 X = S
8130  RETURN
8200  FOR I = 10 TO 20
8210  HTAB 1: VTAB I + 1: PRINT  TAB(
      39);" "
8220  NEXT I
8230  HTAB 1: VTAB 11
8240  RETURN
9000 D$ =  CHR$ (4)
9010  PRINT "INTRODUZCA EL DISCO
      DE DATOS Y PULSE  UNA TECLA
      : ";: GET N$
9015  PRINT
9020  PRINT D$;"OPEN FRECUENCIA"
9030  PRINT D$;"READ FRECUENCIA"
9040  FOR I = 1 TO 26
9050  INPUT E(I)
```

```
9060  NEXT I
9070  PRINT D$;"CLOSE FRECUENCIA"

9080  PRINT D$;"OPEN TRANSICION"
9090  PRINT D$;"READ TRANSICION"
9100  FOR X = 1 TO 26
9110  FOR Y = 1 TO 26
9120  INPUT T(X,Y)
9130  NEXT Y
9140  NEXT X
9150  PRINT D$;"CLOSE  TRANSICION
      "
9160  RETURN
9999  REM   FIN
```

HILL

```
10  REM  **** HILL ****
12  DATA  1,9,21,15,3,19,0,7,23,1
     1,5,17,25
15  HOME
20  PRINT : PRINT  TAB( 7);"PROGR
     AMA DE CIFRADO 'HILL'"
21  PRINT  TAB( 7);"-------------
     -------------"
30  VTAB 5: INPUT "MODO: ";M$
40  IF M$ = "0" THEN  GOTO 9999
50  IF M$ <  > "C" AND M$ <  > "D
     " THEN  GOTO 30
100  VTAB 7: INPUT "MATRIZ: ";A,B
     ,C,D
130 L = A * D - B * C
133  GOSUB 1000
137 DET = L
140  IF L <  > 0 THEN  GOTO 180
150  PRINT : PRINT "NO EXISTE MAT
     RIZ INVERSA"
160  GOTO 100
180  IF (L / 2) >  INT (L / 2) AND
     (L / 13) >  INT (L / 13) THEN
      GOTO 220
190  PRINT : PRINT "EL DETERMINAN
     TE NO ES ADECUADO"
200  GOTO 100
220  VTAB 9: INPUT "TEXTO: ";T$
240  IF  LEFT$ (T$,1) = "0" THEN
      GOTO 9999
260  FOR I = 1 TO  LEN (T$)
270  IF I >  LEN (T$) THEN  GOTO
     330
275 T1$ =  MID$ (T$,I,1)
280  IF T1$ >  = "A" AND T1$ <  =
     "Z" THEN  GOTO 330
290 R$ = ""
300  IF I > 1 THEN R$ =  LEFT$ (T
     $,I - 1)
310  IF I <  LEN (T$) THEN R$ = R
     $ +  RIGHT$ (T$, LEN (T$) -
     I)
320 T$ = R$
325  GOTO 270
330  NEXT I
340 LT =  LEN (T$)
350  IF LT > 1 THEN  GOTO 380
360  GOTO 220
380  IF (LT / 2) =  INT (LT / 2) THEN
      GOTO 410
390 T$ = T$ + "Z"
400 LT = LT + 1
410  PRINT : PRINT "TTEXTO: ";T$
415 CA =  ASC ("A") - 1
416  DIM TN$(LT)
417  FOR N = 1 TO LT
418 TN$(N) =  MID$ (T$,N,1)
419  NEXT N
420  IF M$ = "C" THEN  GOTO 500
425  FOR I = 1 TO 25 STEP 2
426  READ J
427  IF I = DET THEN R = J
428  NEXT I
430 I = A
433 A = D
437 D = I
440 B =  - B
445 C =  - C
450 L = A * R
453  GOSUB 1000
457 A = L
460 L = B * R
463  GOSUB 1000
464 B = L
465 L = C * R
466  GOSUB 1000
467 C = L
470 L = D * R
473  GOSUB 1000
477 D = L
480  PRINT
490  PRINT "MATRIZ INVERSA: ";A;"
     ,";B;",";C;",";D
500  PRINT
510  FOR I = 1 TO LT STEP 2
520 L1 =  ASC (TN$(I)) - CA
530 L2 =  ASC (TN$(I + 1)) - CA
540 L = A * L1 + B * L2
550  GOSUB 1000
560  PRINT  CHR$ (LL + CA);
570 L = C * L1 + D * L2
580  GOSUB 1000
590  PRINT  CHR$ (LL + CA);
600  NEXT I
610  GOTO 9999
1000  IF L >  = 0 AND L < 26 THEN
```

```
      GOTO 1040
1010  IF L < 0 THEN L = L + 26
1020  IF L >  = 26 THEN L = L - 2
     6
1030  GOTO 1000
```

```
1040 LL = L
1050  IF L = 0 THEN LL = 26
1060  RETURN
9999  REM  FIN
```

GRONSFELD

```
10  REM  **** GRONSFELD ****
15  HOME
20  PRINT : PRINT  TAB( 5);"PROGR
     AMA DE CIFRADO 'GRONSFELD'"
25  PRINT  TAB( 5);"-------------
     ------------------"
30  VTAB 5: INPUT "MODO: ";M$
40  IF M$ = "0" THEN  GOTO 9999
45  IF M$ <  > "C" AND M$ <  > "D
     " THEN  GOTO 30
50  PRINT : INPUT "NUMERO CLAVE:
     ";NC$
60 LNC =  LEN (NC$)
65  IF LNC <  = 1 THEN  PRINT  CHR$
     (7): CLEAR : GOTO 30
70  DIM K(LNC)
80  FOR I = 1 TO LNC
90 N1C$ =  MID$ (NC$,I,1)
100  IF N1C$ < "0" OR N1C$ > "9" THEN
      CLEAR : GOTO 30
110 K(I) =  VAL (N1C$)
120  NEXT I
130  POKE 34,8
140  PRINT : INPUT "TEXTO: ";T$
160  IF  LEFT$ (T$,1) = "0" THEN
      GOTO 9999
170 LT =  LEN (T$)
180  IF LT > 0 THEN  GOTO 200
190  GOTO 150
200  PRINT : PRINT "TEXTO : ";T$
210  PRINT
220 CS =  ASC (" ")
230 C1 =  ASC ("A")
```

```
240 CZ =  ASC ("Z")
260 K = 0
265  DIM TM$(LT)
270  FOR I = 1 TO LT
280 TM$(I) =  MID$ (T$,I,1)
290  NEXT I
295  IF M$ = "D" THEN  GOTO 410
300  FOR I = 1 TO LT
310  IF TM$(I) <  > " " THEN  GOTO
     340
320 L = CS
330  GOTO 380
340 K = K + 1
350  IF K > LNC THEN K = 1
360 L =  ASC (TM$(I)) + K(K)
370  IF L > CZ THEN L = L - 26
380  PRINT  CHR$ (L);
390  NEXT I
400  GOTO 9999
410 K = 0
420  FOR I = 1 TO LT
430  IF TM$(I) <  > " " THEN  GOTO
     460
440 L = CS
450  GOTO 500
460 K = K + 1
470  IF K > LNC THEN K = 1
480 L =  ASC (TM$(I)) - K(K)
490  IF L < C1 THEN L = L + 26
500  PRINT  CHR$ (L);
510  NEXT I
9999  POKE 34,0: END : REM  FIN
```

BIFIDO

```
10  REM   **** BIFID ****
15  HOME
20  PRINT : PRINT  TAB( 6);"PROGR
     AMA DE CIFRADO 'BIFID'"
21  PRINT  TAB( 6);"-------------
     --------------"
30  VTAB 5: PRINT "MODO : ";
35  INPUT "";M$
40  IF M$ = "0" THEN  GOTO 9999
```

```
45  IF M$ <  > "C" AND M$ <  > "D
     " THEN  GOTO 30
50  PRINT : PRINT "PALABRA CLAVE
     : ";
55  INPUT "";PC$
60  IF  LEN (PC$) < 2 THEN  GOTO
     30
100  DIM A(25)
110  DIM L(25)
```

```
115 CA =  ASC ("A") - 1
120 A = 0
130  FOR I = 1 TO  LEN (PC$)
140 P1C$ =  MID$ (PC$,I,1)
145 C =  ASC (P1C$) - CA
150  IF L(C) > 0 THEN  GOTO 190
160 A = A + 1
170 A(A) = C
180 L(C) = A
190  NEXT I
200  FOR I = 1 TO 25
210  IF L(I) > 0 THEN  GOTO 250
220 A = A + 1
230 A(A) = I
240 L(I) = A
250  NEXT I
260  PRINT : PRINT "ALFABETO ALTE
     RADO : "
270  PRINT
280  FOR I = 0 TO 4
290  FOR J = 1 TO 5
300  VTAB 9 + I: HTAB 25 + J: PRINT
      CHR$ (A(I * 5 + J) + CA);
310  NEXT J
320  NEXT I
330  POKE 34,15
335  PRINT : PRINT "LONGITUD DEL
     BLOQUE : ";
340  INPUT "";B
345  IF B = 0 THEN  GOTO 9999
350  IF B > 1 AND B =  INT (B) THEN
      GOTO 380
360  GOTO 335
380  PRINT : PRINT  TAB( 4);"LONG
     ITUD DEL BLOQUE : ";B
385  DIM B(2 * B)
390  PRINT : PRINT "TEXTO : ";
400  INPUT "";T$
405  IF  LEFT$ (T$,1) = "0" THEN
      GOTO 9999
410  FOR I = 1 TO  LEN (T$)
420  IF I >  LEN (T$) THEN  GOTO
     490
430 T1$ =  MID$ (T$,I,1)
431  IF T1$ >  = "A" AND T1$ <  =
     "Y" THEN  GOTO 490
440 R$ = ""
450  IF I > 1 THEN R$ =  LEFT$ (T
     $,I - 1)
460  IF I <  LEN (T$) THEN R$ = R
     $ +  RIGHT$ (T$, LEN (T$) -
     I)
470 T$ = R$
480  GOTO 420
490  NEXT I
500 LT =  LEN (T$)
510  IF LT > 1 THEN  GOTO 540
520  GOTO 400
540  PRINT : PRINT "TEXTO : ";T$
549  PRINT
550  DIM TM$(LT)
551  FOR I = 1 TO LT
552 TM$(I) =  MID$ (T$,I,1)
553  NEXT I
560  IF M$ = "D" THEN  GOTO 720
570  FOR I = 1 TO LT STEP B
580 T = B - 1
590  IF I + T > LT THEN T = LT -
     I
600  FOR J = 0 TO T
610 L =  ASC (TM$(I + J)) - CA
620 A = L(L)
630 B(J + 1) =  INT ((A - 1) / 5)
      + 1
640 B(J + T + 2) = A - 5 * (B(J +
     1) - 1)
650  NEXT J
660  FOR J = 0 TO 2 * T STEP 2
670 C = (B(J + 1) - 1) * 5 + B(J +
     2)
680  PRINT  CHR$ (A(C) + CA);
690  NEXT J
700  NEXT I
710  GOTO 9999
720  FOR I = 1 TO LT STEP B
730 T = B - 1
740  IF I + T > LT THEN T = LT -
     I
750  FOR J = 0 TO T
760 C =  ASC (TM$(I + J)) - CA
770 A = L(C)
780 B(J * 2 + 1) =  INT ((A - 1) /
     5) + 1
790 B(J * 2 + 2) = A - 5 * (B(J *
     2 + 1) - 1)
800  NEXT J
810  FOR J = 0 TO T
820 L = (B(J + 1) - 1) * 5 + B(J +
     T + 2)
830  PRINT  CHR$ (A(L) + CA);
840  NEXT J
850  NEXT I
9999  POKE 34,0: END : REM  FIN
```

ANALISIS. ¿QUE CIFRADO?

```
10  REM  **** ANALISIS QUE CIFRAD
     O ? ****
15  HOME
20  PRINT : PRINT "PROGRAMA DE AN
     ALISIS 'QUE CIFRADO'"
30  PRINT : INPUT "TEXTO: ";T$
```

```
45  IF  LEFT$ (T$,1) = "0" THEN  GOTO
    9999
50  FOR I = 1 TO  LEN (T$)
60  IF I >  LEN (T$) THEN  GOTO 1
    30
70 T1$ =  MID$ (T$,I,1)
75  IF T1$ >  = "A" AND T1$ <  =
    "Z" THEN  GOTO 130
80 R$ = ""
90  IF I > 1 THEN R$ =  LEFT$ (T$
    ,I - 1)
100  IF I <  LEN (T$) THEN R$ = R
    $ +  RIGHT$ (T$, LEN (T$) -
    I)
110 T$ = R$
120  GOTO 60
130  NEXT I
140 LT =  LEN (T$)
150  IF LT > 25 THEN  GOTO 180
160  GOTO 30
180 CA =  ASC ("A") - 1
190  DIM F(27)
200  FOR I = 1 TO LT
210 F( ASC ( MID$ (T$,I,1)) - CA)
     = F( ASC ( MID$ (T$,I,1)) -
    CA) + 1
220  NEXT I
230 M = 0
235 OL = 0
240  FOR I = 1 TO 26
250  IF F(I) > M THEN M = F(I)
255  IF F(I) = 0 THEN OL = 1
260  NEXT I
270  HOME
280  HTAB 5
290  VTAB 14: PRINT "ABCDEFGHIJKL
    MNOPQRSTUVWXYZ"
350  VTAB 1: HTAB 1: PRINT "20% "
    : PRINT : PRINT : PRINT "15%
     ": PRINT : PRINT : PRINT "1
    0% ": PRINT : PRINT : PRINT
    " 5% ": PRINT : PRINT : PRINT
    " 0% "
370  FOR I = 1 TO 26
380 H = F(I) / LT
390  IF H > .2 THEN H = .2
395  HTAB (4 + I): VTAB (13 - (60
     * H) + .5): INVERSE : PRINT
    " ": NORMAL
397  NEXT I
400  GET A$
410  HOME
420 S = 0
430  FOR I = 1 TO 26
440 S = S + F(I) * (F(I) - 1)
450  NEXT I
460 IC = S / (LT * (LT - 1))
470  PRINT : PRINT "INDICE DE COI
    NCIDENCIA DE ": PRINT : PRINT
    "LETRAS AISLADAS = ";IC
480  DIM P(702)
490 L1 = LT
500  IF L1 / 2 >  INT (L1 / 2) THEN
    L1 = L1 - 1
510  FOR I = 1 TO L1 STEP 2
520 P = ( ASC ( MID$ (T$,I,1)) -
    CA) * 26 +  ASC ( MID$ (T$,I
     + 1,1)) - CA
530 P(P) = P(P) + 1
540  NEXT I
550 S = 0
560  FOR I = 1 TO 676
570 S = S + P(I) * (P(I) - 1)
580  NEXT I
590 IP = S / (L1 * (L1 - 1))
600  PRINT : PRINT "INDICE DE COI
    NCIDENCIA DE": PRINT : PRINT
    "PARES DE LETRAS = ";IP
9999  REM  FIN
```

ANALISIS GRONSFELD

```
10  REM  ANALISIS GRONSFELD"
20  PRINT "INTRUDUZCA UN DISCO CO
    N DATOS Y          PULSE UNA
    TECLA"
25  GET A$
26  PRINT
28  PRINT  CHR$ (4);"OPEN FRECUEN
    CIA"
30  PRINT  CHR$ (4);"READ FRECUEN
    CIA"
32  FOR I = 1 TO 26
34  INPUT E(I)
36  NEXT
38  PRINT  CHR$ (4)"CLOSE FRECUEN
    CIA"
40  PRINT  CHR$ (4);"OPEN TRANSIC
    ION"
42  PRINT  CHR$ (4);"READ TRANSIC
    ION"
44  FOR I = 1 TO 26
46  FOR J = 1 TO 26
48  INPUT T(I,J)
50  NEXT : NEXT
52  PRINT  CHR$ (4)"CLOSE TRANSIC
    ION"
70  HOME
80  PRINT "PROGRAMA DE ANALISIS G
    RONSFELD"
90  HTAB 2: VTAB 2
100  INPUT "TEXTO: ";T$
```

```
105  IF  LEFT$ (T$,1) = "0" THEN
      GOTO 9999
110  FOR I = 1 TO  LEN (T$)
120  IF I >  LEN (T$) THEN  GOTO
     190
125 T1$ =  MID$ (T$,I,1)
130  IF T1$ >  = "A" AND T1$ <  =
     "Z" THEN  GOTO 190
140 R$ = ""
150  IF I > 1 THEN R$ =  LEFT$ (T
     $,I - 1)
160  IF I <  LEN (T$) THEN R$ = R
     $ +  RIGHT$ (T$, LEN (T$) -
     I)
170 T$ = R$
180  GOTO 120
190  NEXT I
210 LT =  LEN (T$)
220  IF LT > 10 THEN  GOTO 250
230  PRINT "TEXTO CORTO"
240  GOTO 100
250  PRINT "TEXTO: ";T$
255 CA =  ASC ("A") - 1
260  FOR QW = 1 TO LT:F$(QW) = "
     ":D(QW) = 1: NEXT
280 NR = 0
290  HOME
295  PRINT "FACTORES DE REPETICIO
     N:"
300  GOSUB 5000
431  PRINT "HAY ";NR;" REPETICION
     ES."
740  FOR I = 1 TO LT
750 L =  ASC ( MID$ (T$,I,1)) - C
     A
760  LET C(L) = C(L) + 1
770  NEXT I
780 S = 0
790  FOR I = 1 TO 26
800 S = S + C(I) * (C(I) - 1)
810  NEXT I
820 IC = S / (LT * (LT - 1))
830  PRINT "INDICE DE COINCIDENCI
     A: ";IC
840  INPUT "LONGITUD DE LA CLAVE
     A BUSCAR: ";KL
850  IF KL = 0 THEN  GOTO 9999
860  IF KL < 2 OR KL > LT / 2 OR
     KL >  INT (KL) GOTO 840
920  PRINT "LONGITUD DE LA CLAVE:
      ";KL
930  FOR QW = 1 TO 25: FOR WQ = 1
      TO 10:P(QW,WQ) = 0: NEXT :K
     (QW) = 0: NEXT
931  FOR QW = 1 TO LT:F$(QW) = "
     ": NEXT
935  FOR I = 1 TO KL:K(I) =  - 1:
      NEXT
940  FOR I = 1 TO 26
950 C(I) = C(I) / LT
960  NEXT I
961  PRINT "PULSE UNA TECLA"
962  GET A$
965  HOME
969  GOTO 7000
970  FOR C = 1 TO KL
980  GOSUB 8000
990  NEXT C
1140 NC = 0
1150 NC = NC + 1
1160  IF LT / (NC * KL) > 15 THEN
      GOTO 1150
1165 CL = NC * KL
1167 NR = LT / CL
1260  GOSUB 8200
1270  HTAB 1: VTAB 23: PRINT "PUL
     SE A,B,C,D,E,F,K,N,P,S,T,W,0
     .";
1280  GET R$
1290  PRINT "    ";
1305  IF R$ = "A" THEN  GOTO 7000

1310  IF R$ <  > "B" THEN  GOTO 1
     380
1320  GOSUB 8300
1330 K(C) =  - 1
1333  FOR I = 1 TO 10
1335 P(C,I) = 0
1337  NEXT I
1340  FOR I = C TO LT STEP KL
1350 F$(I) = " "
1360  NEXT I
1370  GOTO 1260
1380  IF R$ <  > "C" THEN  GOTO 1
     410
1390  REM
1400  GOTO 1270
1410  IF R$ <  > "D" THEN  GOTO 1
     450
1420  FOR QW = 1 TO LT:F$(QW) = "
     ": NEXT
1430  FOR I = 1 TO KL
1431 K(I) =  - 1
1432  NEXT I
1435  FOR QW = 1 TO 25: FOR WQ =
     1 TO 10:P(QW,WQ) = 0: NEXT :
      NEXT
1440  GOTO 1260
1450  IF R$ <  > "E" THEN  GOTO 1
     500
1460  GOSUB 9000: PRINT "LETRA? "
     ;: GET L$
1465  IF L$ = "0" THEN  GOTO 9999
1470  IF  LEN (L$) <  > 1 OR L$ <
     "A" OR L$ > "Z" THEN  GOTO 1
     460
1480  PRINT L$;": ";E( ASC (L$) -
     CA)
1490  GOTO 1270
1500  IF R$ <  > "F" THEN  GOTO 1
     550
1505 Z = 2
1510  FOR C = 1 TO KL
1520  IF K(C) < 0 THEN  IF (F$(KL
      + C - 1) <  > " ") OR (F$(C
      + 1) <  > " ") THEN  GOSUB
```

```
    8000: GOSUB 8200
1530  NEXT C
1533 Z = Z - 1
1536  IF Z >  = 0 THEN  GOTO 1510

1537  FOR I = 1 TO KL
1538  IF K(I) < 0 THEN  GOTO 1505

1539  NEXT I
1540  GOTO 1260
1550  IF R$ <  > "K" THEN  GOTO 1
    580
1560  HOME
1570  GOTO 840
1580  IF R$ <  > "N" THEN  GOTO 1
    620
1590  GOSUB 8300
1600  GOSUB 8000
1610  GOTO 1260
1620  IF R$ = "P" GOTO 7230
1625  IF R$ <  > "S" THEN  GOTO 1
    660
1630  HOME
1631  GOSUB 9000: PRINT "CLAVE: "
    ;
1632  FOR I = 1 TO KL
1633  PRINT K(I);
1634  NEXT I
1640  PRINT : PRINT : FOR I = 1 TO
    LT: PRINT F$(I);: NEXT : PRINT

1650  GOTO 9999
1660  IF R$ <  > "T" THEN  GOTO 1
    740
1665  GOSUB 9000
1670  INPUT "LETRAS ";L$
1675  IF L$ = "0" THEN  GOTO 9999
1680  IF  LEN (L$) <  > 2 GOTO 16
    70
1690 L1 =  ASC ( LEFT$ (L$,1)) -
    CA
1700 L2 =  ASC ( RIGHT$ (L$,1)) -
    CA
1710  IF L1 < 1 OR L1 > 26 OR L2 <
    1 OR L2 > 26 THEN  GOTO 1670

1715  HTAB 20: VTAB 22
1720  PRINT L$": "T(L1,L2)
1730  GOTO 1270
1740  IF R$ <  > "W" THEN  GOTO 1
    800
1750  GOSUB 8300
1755  GOSUB 9000
1760  INPUT "CLAVE ";D
1770  IF D < 0 OR D > 9 OR D >  INT
    (D) THEN  GOTO 1760
1780  GOSUB 8170
1790  GOTO 1260
1800  IF R$ = "0" THEN  GOTO 9999

1805  HTAB 33: VTAB 23
1810  PRINT "?"; CHR$ (7)
1820  GOTO 1270

5000  FOR I = 2 TO 6
5015  FOR K = 1 TO LT - 2 * I + 1

5020  FOR J = I + K TO LT - I + 1

5030  IF  MID$ (T$,K,I) =  MID$ (
    T$,J,I) THEN  GOSUB 6000
5040  NEXT : NEXT : NEXT
5050  RETURN
6000 D = J - K
6005 NR = NR + 1
6010  PRINT NR". "K","J" " MID$ (
    T$,K,I);" DIST="D" DIV";
6030 W = D: IF D > 10 THEN W = 10

6040  FOR DI = 2 TO W
6050  IF D / DI =  INT (D / DI) THEN
    PRINT "-";DI;
6060  NEXT
6070  PRINT : RETURN
7000  GOSUB 9000: INPUT "PALABRA
    PROBABLE: ";W$
7010  IF W$ = "0" THEN  GOTO 9999

7020  IF W$ = "" GOTO 970
7030 LW =  LEN (W$)
7040  FOR QW = 1 TO 25:O(QW) = 0:
    NEXT
7050  FOR I = 1 TO LW
7060 W(I) =  ASC ( MID$ (W$,I,1))
    - CA
7065  IF W(I) < 1 OR W(I) > 26 THEN
    GOTO 7000
7070  NEXT I
7080 NP = 0
7100  FOR I = 0 TO LT - LW - 1
7110  FOR J = 1 TO LW
7120 L =  ASC ( MID$ (T$,I + J,1)
    ) - CA
7130  FOR K = 0 TO 9
7140 N = L - K
7150  IF N < 1 THEN N = N + 26
7160  IF N = W(J) THEN  GOTO 7190

7170  NEXT K
7180  GOTO 7220
7190  NEXT J
7200 NP = NP + 1
7210 O(NP) = I + 1
7220  NEXT I
7230  HOME
7235  IF NP > 0 THEN  GOTO 7260
7240  PRINT "'";W$"' NO PUEDE SER
    ."
7250  GOTO 7000
7260  PRINT "PUEDE ESTAR EN ";NP;
    " SITIOS. "
7270  FOR I = 1 TO NP
7280  PRINT I". CARACTER "O(I)"-"
    ;
7290  PRINT  MID$ (T$,O(I),LW)
7330  NEXT I
7335  PRINT
```

```
7340  INPUT "NUMERO DE OPCION: ";
    O
7345  IF O = 0 THEN  GOTO 9999
7350  IF O < 1 OR O > NP OR O >  INT
    (O) THEN  GOTO 7340
7360 P = O(O)
7370 C = P - KL *  INT (P / KL)
7380  IF C = 0 THEN C = KL
7390  FOR J = 0 TO LW - 1
7400 L =  ASC ( MID$ (T$,P + J,1)
    ) - CA
7410  FOR K = 0 TO 9
7420 N = L - K
7430  IF N < 1 THEN N = N + 26
7440  IF N <  > W(J + 1) THEN  NEXT
    K
7450 D = K
7455  GOSUB 8170
7460 C = C + 1
7470  IF C > KL THEN C = C - KL
7480  NEXT J
7490  HOME
7500  GOTO 1140
8000 B = 999
8010 D = 0
8020  FOR K = 0 TO 9
8025  IF P(C,K + 1) <  > 0 THEN  GOTO
    8160
8030 T = 0
8040 N = L - K
8050  IF N < 1 THEN N = N + 26
8060 T = T + (LT / KL) *  ABS (E(
    N) - C(L))
8065  FOR J = 0 TO LT - KL STEP K
    L
8070 P = C + J
8080 L =  ASC ( MID$ (T$,P,1)) -
    CA
8100  IF P > 1 AND F$(P + 1) <  >
    " " THEN T = T - T( ASC (F$(
    P - 1)) - CA,N)
8110  IF P < L AND F$(P + 1) <  >
    " " THEN T = T - T(N, ASC (F
    $(P + 1)) - CA)
8120  NEXT J
8130  IF T > B THEN  GOTO 8160
8140 B = T
8150 D = K
8160  NEXT K
8170 K(C) = D
8175 P(C,D + 1) = 1
8180  FOR I = C TO LT STEP KL
8182 L =  ASC ( MID$ (T$,I,1)) -
    CA - D
8184  IF L < 1 THEN  LET L = L +
    26
8186  LET F$(I) =  CHR$ (L + CA)
8188  NEXT I
8190  RETURN
8200  HTAB 7: VTAB 1: FOR I = 1 TO
    KL: PRINT  RIGHT$ ( STR$ (I)
    ,1);: NEXT
8201  VTAB 4
8205  FOR I = 0 TO NR - 1
8210  HTAB 7
8211  FOR QW = CL * I + 1 TO CL *
    (I + 1): PRINT F$(QW);: NEXT
    : PRINT
8220  NEXT I
8225  IF LT / CL >  INT (LT / CL)
     THEN  VTAB 4 + I: HTAB 7: FOR
    QW = CL * I + 1 TO LT: PRINT
    F$(QW);: NEXT : PRINT
8226  VTAB 2
8235  HTAB 1
8236  PRINT "CLAVE=";
8240  FOR J = 1 TO KL
8250  PRINT  LEFT$ ( STR$ (K(J)),
    1);
8260  NEXT J
8265  PRINT
8280  RETURN
8300  GOSUB 9000: INPUT "QUE COLU
    MNA?";C
8310  IF C = 0 THEN  GOTO 9999
8320  IF C < 1 OR C > KL OR C >  INT
    (C) THEN  GOTO 8300
8330  RETURN
9000  HTAB 1: VTAB 22: PRINT "

              ": VTAB 22: RETURN

9999  REM  FIN
```

SEGURO

```
10  REM  **** SEGURO ****
15  HOME
20  PRINT : PRINT "PROGRAMA DE CI
     FRADO SEGURO"
21  PRINT "----------------------
     ----"
30  VTAB 5: INPUT "MODO: ";M$
50  IF  LEFT$ (M$,1) = "O" THEN  GOTO
     9999
60  IF M$ = "C" OR M$ = "D" THEN
      GOTO 90
70  GOTO 30
90  VTAB 7: INPUT "NUMERO CLAVE:
     ";K
110  IF K = 0 THEN  GOTO 9999
130  IF K > 0 AND K < 65536 AND K
      =  INT (K) THEN  GOTO 170
140  GOTO 90
```

```
170  VTAB 9: INPUT "PALABRA CLAVE
     : ";K$
190  IF  LEFT$ (K$,1) = "0" THEN
      GOTO 9999
200 LK =  LEN (K$)
210  IF LK > 0 THEN  GOTO 240
220  GOTO 170
240  DIM A(25)
250  DIM L(25)
260 CA =  ASC ("A") - 1
270 A = 0
280  FOR I = 1 TO LK
285 KM$ =  MID$ (K$,I,1)
290 C =  ASC (KM$) - CA
300  IF C < 1 OR C > 25 THEN  GOTO
     220
310  IF L(C) > 0 THEN  GOTO 350
320 A = A + 1
330 A(A) = C
340 L(C) = A
350  NEXT I
360  FOR I = 1 TO 25
370  IF L(I) > 0 THEN  GOTO 410
380 A = A + 1
390 A(A) = I
400 L(I) = A
410  NEXT I
420  PRINT : PRINT "ALFABETO ALTE
     RADO: "
430  FOR I = 0 TO 4
440  FOR J = 1 TO 5
450  VTAB 11 + I: HTAB 25 + J: PRINT
      CHR$ (A(I * 5 + J) + CA)
460  NEXT J
470  NEXT I
480  VTAB 17: INPUT "TEXTO: ";T$
500  IF  LEFT$ (T$,1) = "0" THEN
      GOTO 9999
510  FOR I = 1 TO  LEN (T$)
520  IF I >  LEN (T$) THEN  GOTO
     590
530 T1$ =  MID$ (T$,I,1)
535  IF T1$ >  = "A" AND T1$ <  =
     "Z" THEN  GOTO 590
540 R$ = ""
550  IF I > 1 THEN R$ =  LEFT$ (T
     $,I - 1)
560  IF I <  LEN (T$) THEN R$ = R
     $ +  RIGHT$ (T$, LEN (T$) -
     I)
570 T$ = R$
580  GOTO 520
590  NEXT I
600 LT =  LEN (T$)
610  IF LT > 0 THEN  GOTO 640
620  GOTO 480
640  PRINT : PRINT "TEXTO: ";T$
646  IF M$ = "C" THEN  PRINT : PRINT
     "TEXTO CIFRADO: ";: GOTO 648

647  IF M$ = "D" THEN  PRINT : PRINT
     "TEXTO DESCIFRADO: ";
648  DIM TM$(LT)
649 W =  RND ( - K):W = 0
650  FOR M = 1 TO LT
651 TM$(M) =  MID$ (T$,M,1)
652  NEXT M
660  IF M$ = "D" THEN  GOTO 760
670  FOR I = 1 TO LT
680 C =  ASC (TM$(I)) - CA
690 X =  INT ((C - 1) / 5) +  INT
     (5 *  RND (1)) + 2
700  IF X > 5 THEN X = X - 5
710 Y = C -  INT ((C - 1) / 5) *
     5 +  INT (5 *  RND (1)) + 1
720  IF Y > 5 THEN Y = Y - 5
730  PRINT  CHR$ (L((X - 1) * 5 +
     Y) + CA);
740  NEXT I
750  GOTO 9999
760  FOR I = 1 TO LT
770 C = A( ASC (TM$(I)) - CA)
780 X =  INT ((C - 1) / 5) -  INT
     (5 *  RND (1))
790  IF X < 1 THEN X = X + 5
800 Y = C -  INT ((C - 1) / 5) *
     5 -  INT (5 *  RND (1)) - 1
810  IF Y < 1 THEN Y = Y + 5
820  PRINT  CHR$ ((X - 1) * 5 + Y
      + CA);
830  NEXT I
9999  REM  FIN
```

CREACION DE DATOS

```
6  HOME
10  PRINT : PRINT "PROGRAMA DE CR
     EACION DE DATOS"
15  PRINT "----------------------
     -------"
20  PRINT : PRINT "ESCRIBA LA FRE
     CUENCIA DE CADA LETRA"
25  PRINT : PRINT "SEGUN SE PIDA.
     "
30  DIM E(26)
40  FOR I = 1 TO 26
50  INPUT "";E(I)
60  NEXT I
70  PRINT : PRINT "ESCRIBA AHORA
     LOS DATOS DE TRANSICION "
75  PRINT : PRINT "PARA CADA PAR
     DE LETRAS"
80  DIM T(26,26)
```

```
90  FOR I = 1 TO 26
100  FOR J = 1 TO 26
110  INPUT "";T(I,J)
120  NEXT J
125  PRINT
130  NEXT I
140  PRINT : PRINT "PRINT INTRODU
     ZCA EL DISCO EN QUE QUIERA"
145  PRINT : PRINT "SALVAR LOS DA
     TOS, Y PULSE UNA TECLA"
146  GET A$
150  PRINT  CHR$ (4);"OPEN FRECUE
     NCIA"
155  PRINT  CHR$ (4);"WRITE FRECU
     ENCIA"
160  FOR I = 1 TO 26
170  PRINT E(I)
180  NEXT I
200  PRINT  CHR$ (4);"CLOSE FRECU
     ENCIA"
210  PRINT  CHR$ (4);"OPEN TRANSI
     CION"
215  PRINT  CHR$ (4);"WRITE TRANS
     ICION"
220  FOR I = 1 TO 26
225  FOR J = 1 TO 26
230  PRINT T(I,J)
240  NEXT J
250  NEXT I
270  PRINT  CHR$ (4);"CLOSE TRANS
     ICION"
```

Apéndice 5

Bibliografía

Son pocos los libros escritos sobre el tema de la criptografía. Afortunadamente, la mayor parte de ellos son muy buenos y cada uno trata esta materia de forma muy particular. La siguiente lista te dará una idea de aquellos libros en los que podrás interesarte en el futuro.

1. *The Codebreakers*, de David Khan, Weidenfeld y Nicholson, 1973.

   Es la historia de la criptografía escrita de forma amena y comprensible. Lee la versión íntegra de tapa dura. Es fascinante.

2. *Cryptography-A Primer*, de Alan Konheim, Wiley, 1981.

   Hasta el momento de escribir éste, es el mejor libro de referencia disponible sobre la teoría matemática de la criptografía. Introdúcete en él si tienes conocimientos sólidos de matemáticas.

Estos dos libros son los primeros de la bibliografía porque los he tomado como referencia. El siguiente grupo es más accesible para aquellos entusiastas que no tengan conocimientos de altas matemáticas.

3. *Elementary Cryptanalysis-A Mathematical Approach*, por Abraham Sinkov, publicado por la Asociación de Matemáticos de América en 1966.

Este es el único libro de la lista del cual el autor sabe que ha sido escrito por un criptoanalista matemático profesional (Sinkov trabajó en los servicios de inteligencia americanos durante la Segunda Guerra Mundial). El libro trata los cifrados monoalfabéticos, polialfabéticos, poligráficos y de transposición. Los apéndices contienen estadísticas útiles y tiene un suplemento con programas en BASIC para cifrar y descifrar mensajes, además de hacer análisis simples de frecuencias. También es una buena bibliografía para aquellos que estén dispuestos a recordar las matemáticas elementales.

4. *Cryptanalysis*, por Helen Fonche Gaines. Publicado por Dover Publications, 1956.

Trata los mismos cifrados que el libro de Sinkov, pero da las soluciones con métodos manuales. Este libro se suele llamar "la Biblia del criptoanalista aficionado" —un título bien merecido.

5. *Cryptanalysis for Microcomputers*, por Caxtin C. Foster, publicado por Hayden en 1982.

Trata el mismo tipo de cifrados que Sinkov y Gaines, pero también incluye varios cifrados por fraccionamiento como el "Bífido" y otros. Tiene excelentes apéndices que dan las frecuencias para los textos en inglés (también incluye listados en BASIC para el Commodore de cifrado, descifrado y análisis). Los métodos de análisis no utilizan las probabilidades de contacto de este libro, pero hay alguno con base matemática. Recomendado para todos los criptoanalistas informáticos.

6. *Codes, Ciphers and Computers-An Introduction to Information Security*, por Bruce Bosworth. Publicado por Hayden en 1982.

Trata los códigos y los cifrados, pero no incluye demasiado sobre cifrados poligráficos y polialfabéticos. Tiene unos capítulos introductorios excelentes sobre estándares de datos cifrados y recientes desarrollos también llamados "cifrados de claves públicas". Trata más sobre los cifrados aplicados a los sistemas de comunicaciones por ordenador que de los cifrados como tales. Es muy claro y asimilable por el gran número de ejemplos que contiene.

El próximo grupo de libros se refiere a la solución de cifrados por métodos manuales y a los textos introductorios más elementales.

7. *Codes and Ciphers*, por Frank Higenbottom. Publicado por EUP en 1973.

Este libro es parte de la famosa serie "Aprenda usted mismo". Tiene un excelente capítulo de introducción a la historia de la criptografía y explica algunas variantes de los cifrados simples. Tiene muchos ejemplos de cifrados por solución manual incluyendo un capítulo con las soluciones de algunos descifrados reales e históricos que fueron descifrados en la época de los

Tudor. El libro también incluye datos de frecuencias para algunas lenguas extranjeras. Tiene mucho valor como libro de consulta.

8. *Secret Language-Communicating in Codes and Ciphers*, por Julian A. Bielewicz. Editado por Jupiter Books en 1976.

Este es un fabuloso libro ilustrado para niños. Explica los mismos tipos de cifrados que el libro de Sinkov, pero también los incluye de otro tipo. Es una buena diversión para jóvenes criptógrafos. Intenta conseguirlo.

9. *Fun With Codes*, por J. V. Reed. Publicado por Pelham Books en 1969.

Solamente considera los cifrados monoalfabéticos, pero da un buen conjunto de reglas con las cuales resolverlos. Es elemental, pero muy comprensible. Tiene una buena información complementaria sobre las frecuencias de las letras y las formas.

Existen otras fuentes al respecto, pero muchos de estos textos no han sido publicados o nunca se podrá disponer de ellos (por ejemplo, los que están bajo secreto militar). Los títulos dados anteriormente se pueden encontrar en algunas librerías, aunque algunos estarán agotados.

Si quieres más títulos, mira la bibliografía de cada uno de esos libros; ¡con ello tendrás más que suficiente para seguir en el tema!

Indice alfabético

ANAYA MULTIMEDIA

Colección «MICROINFORMATICA»

Angell, I. O. y Jones, B. J.: DISEÑO DE GRAFICOS Y VIDEOJUEGOS (incluye cassette).
Beechhold, Henry F.: EL LIBRO DEL HARDWARE. No destape su ordenador personal... sin leer antes este libro.
Birmingham Educational Computing Centre: INTRODUCCION A LA TECNOLOGIA DE LA INFORMACION. PREINFORMATICA.
Bishop, Peter: PROGRAMACION AVANZADA EN BASIC.
Brown, Peter: PASCAL A PARTIR DEL BASIC.
Cavalcoli, Aldo: EL ORDENADOR PERSONAL: COMO ELEGIRLO Y UTILIZARLO.
Coccione, L. y Winter, G.: LOS ORDENADORES NO MUERDEN.
Dachslager, H., Hayashi, M. y Zucker, R.: PROGRAMACION EN BASIC: UN METODO PRACTICO.
Dewhirst, J. y Tennison, R.: TU PRIMER LIBRO DEL ZX SPECTRUM.
D'Opazo, J. y Grupo GOLEM: PROGRAMACION EN LOGO.
Durst, J.: «SPRITES» Y GRAFICOS EN LENGUAJE MAQUINA (ZX SPECTRUM).
Galende Domínguez, F.; Sánchez López, A.; Alfaraz López, M. y Sánchez García, J. A.: COMETAS EN TU MICRO: EL HALLEY. Cálculos de órbitas y parámetros de cometas en BASIC.
Gavin, Maurice: ASTRONOMIA: EL UNIVERSO EN TU ORDENADOR.
Gibbons, John P.: PROGRAMACION AVANZADA DEL COMMODORE 64. Ampliación del BASIC y rutinas gráficas.
Greenwood, Gareth: CODIGOS Y CLAVES SECRETAS. Criptografía en BASIC.
Hammond, R.: EL ORDENADOR Y TUS HIJOS.
Hartnell, Tim: EL LIBRO GIGANTE DE LOS JUEGOS PARA ORDENADOR.
Hartnell, Tim: INTELIGENCIA ARTIFICIAL: CONCEPTOS Y PROGRAMAS.
Hartnell, Tim: EL LIBRO GIGANTE DE LOS JUEGOS PARA ZX SPECTRUM.
Hartnell, Tim, y otros: EL LIBRO GIGANTE DE LOS JUEGOS PARA DRAGON.
Hartnell, Tim: EL SUPERLIBRO DE LOS JUEGOS PARA ORDENADOR.
Heller, R. S. y Martin, C. D.: BITS Y BYTES: INICIACION A LA INFORMATICA.
Hollerbach, Lew: MICROINFORMATICA: CONCEPTOS BASICOS.
Hurley, R.: JUEGOS GRAFICOS DE AVENTURA PARA ZX SPECTRUM.
Johnson, David: DESCUBRE LAS MATEMATICAS CON TU MICRO.
Johnston, J.: MICROS: TAMAÑOS, FORMAS Y SABORES.
Johnston, J.: MICROS: BIPS, PITIDOS Y LUCES.
Johnston, J.: MICROS: MENUS, BUCLES Y RATONES.
Kosniowski, Czes: MATEMATICAS DIVERTIDAS EN BASIC.
Kramer, S.: PROGRAMACION AVANZADA DEL ZX SPECTRUM.
Lacey, Andrew: LIBRO GIGANTE DE LOS JUEGOS PARA MSX.
Núñez, Agustín: PROGRAMACION DEL INTERFACE 1 Y MICRODRIVE.
Otero, M. A.; Pueyo, M. A. y Cajaraville, J. A.: PRIMEROS PASOS EN LOGO. El mundo de la tortuga Fan. Libro del profesor. Libro del alumno.
O'Shea, T. y Self, J.: ENSEÑANZA Y APRENDIZAJE CON ORDENADORES. Inteligencia artificial en educación.
Pentiraro, Egidio: EL ORDENADOR EN EL AULA.
Pritchard, Joe: DESCUBRE TU MSX. Programación y aplicaciones.
Pritchard, Joe: LENGUAJE MAQUINA MSX. Introducción y conceptos avanzados.
Rosso, Vincenzo de: COMO SE PROGRAMAN LOS ORDENADORES.
Sato, T.; Mapstone, P. y Muriel, I.: MSX: GUIA DEL PROGRAMADOR Y MANUAL DE REFERENCIA.
Servello, Fausto: ¿QUE ES LA TELEMATICA?
Snover, S. L. y Spikell, M. A.: JUEGOS MATEMATICOS DE INGENIO EN BASIC.
Thomasson, Don: PROGRAMACION AVANZADA DEL AMSTRAD. Entradas y salidas de la ROM.
Webb, David: LENGUAJE MAQUINA AVANZADO PARA ZX SPECTRUM.
Zaks, Rodnay: EL LIBRO DEL BASIC.

ANAYA MULTIMEDIA

INFORMATICA PERSONAL-PROFESIONAL

EL LIBRO DEL WORDSTAR. *Trucos y recursos.*—Julie Anne Arca.
EL LIBRO DEL ATARI ST. *Manejo, aplicaciones y GEM.*—Jeremy Vine.
EL LIBRO DEL IBM PC, XT, AT. *Programación, uso y aplicaciones.*—Louis E. Frenzel, Jr., Louis E. Frenzel III.
PROGRAMACION EN C. *Introducción y conceptos avanzados.*—M. Waite, S. Prata, D. Martin.
MARKETING Y VENTAS CON LOTUS 1-2-3. *Técnicas comerciales para su microordenador.*—Michael V. Laric, M. Ronald Stiff.
PROGRAMACION DEL Z80.—Rodnay Zaks.
EL LIBRO DEL APPLE IIc. *Programación, uso y aplicaciones.*—Philip Lieberman.
EL LIBRO DEL RS-232.—John Campbell.
EL LIBRO DEL LOTUS 1-2-3. *Desarrollo de aplicaciones profesionales.*—Alan Simpson.
MICROINFORMATICA PARA DIRECTIVOS. *Cómo rentabilizar su ordenador personal-profesional.*—Dick Heiser.
PROGRAMACION GRAFICA EN EL IBM PC.—Dan Illowsky, Michael Abrash.
QUILL. *Tratamiento de textos en el QL.*—F. Simon, C. Spottiswoode, Blueprint.
EASEL. *Gráficos de negocios en el QL*—Alison Spottiswoode, Blueprint.
ABACUS. *Aplicaciones de la hoja electrónica en el QL.*—Clare Spottiswoode, Blueprint.
ARCHIVE. *Manejo de la base de datos en el QL.*—Ian Murray, Blueprint.
MATEMATICAS PARA PROGRAMADORES. *Sistemas de numeración y aritmética binaria.*—William Barden, Jr.
INTRODUCCION AL UNIX SISTEMA V.—Mitchell Waite, Stephen Prata, Donald Martin.
GEOMETRIA DE TORTUGA. *El ordenador como medio de exploración de las matemáticas.*—Harold Abelson, Andrea diSessa.

La criptografía y el criptoanálisis han jugado papeles muy importantes en muchos acontecimientos políticos y diplomáticos de la historia.

CODIGOS Y CLAVES SECRETAS: CRIPTOGRAFIA EN BASIC es una introducción a la criptología para usuarios de microordenadores. A lo largo del libro se describen y analizan las distintas técnicas de cifrado y descifrado de mensajes y se acompañan los programas en BASIC para que el ordenador realice el trabajo repetitivo a partir del ingenio, intuición y destreza del "rompe-claves".

La potencia de los pequeños ordenadores permite tratar con ellos técnicas sofisticadas de cifrado y codificación que permiten una experimentación científica seria de la ciencia de la criptología.

Algunas de las técnicas descritas en CODIGOS Y CLAVES SECRETAS: CRIPTOGRAFIA EN BASIC son:

Sustitución monoalfabética, cifrados en zig-zag, transposición de columnas, de itinerario, cifrados por giro de rejilla (rejilla de Cardano), *fraccionarios* (método Bífido), *poligráficos* (método Hill) *y polialfabéticos* (método Gronsfeld, análisis de Kasiski), *índice de coincidencia, seguridad de una clave.*

El libro contiene además tablas completas con el análisis de frecuencias de letras, digramas y palabras (de 2, 3, 4, 5 letras) y una lista de las palabras más frecuentes en castellano.

Con CODIGOS Y CLAVES SECRETAS: CRIPTOGRAFIA EN BASIC tienes asegurada la entrada a este mundo apasionante en el que tendrás que poner a prueba todos tus reflejos y paciencia.

Con tu ingenio y este libro aprenderás técnicas útiles, te divertirás, desarrollarás tu mente y, quién sabe, ¡tal vez descubras algo que antes no sabías!

El libro contiene versiones completas de todos los programas para SPECTRUM, AMSTRAD, MSX, COMMODORE y APPLE II.

ANAYA MULTIMEDIA

Códigos y Claves Secretas

Gareth Greenwood

AMSTRAD CPC

MÉMOIRE ÉCRITE
MEMORY ENGRAVED
MEMORIA ESCRITA

https://acpc.me/