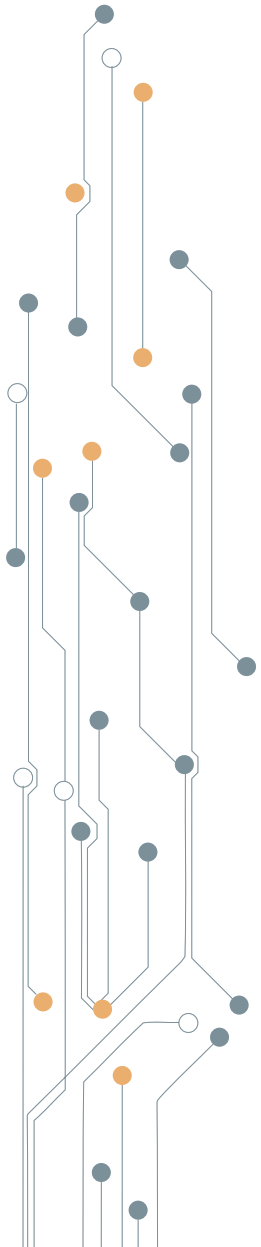
Historia de la criptografía y la cifra clásica

Telefónica EDUCACIÓN DIGITAL

Índice



1. Los inicios de la criptografía

La escítala

Se trata del sistema de cifra más antiguo conocido y data del año 400; es decir, del siglo V antes de Cristo. El pueblo griego espartano conocido como Lacedemonia, comienza a utilizar un artilugio para cifrar información conocido como escítala.

La escítala, mostrada en la figura 1.1, consistía en un bastón en el cual se enrollaba una cinta de cuero y luego se escribía el mensaje secreto de manera longitudinal en los trozos visibles de dicha cinta a lo largo del bastón. Una vez escrito todo el mensaje, se desenrollaba la cinta y los caracteres que en ella aparecían, ya leídos uno a continuación de otro, no guardaban relación alguna con el mensaje original.

Se trata de un sistema de cifra por permutación o transposición de los caracteres. El criptograma tendrá los mismos elementos que el texto en claro, pero estarán distribuidos de otra forma. Hoy en día se sigue usando este tipo de operación en la cifra, pero con bits y bytes.

Figura 3.1. Escítala lacedemonia.

2. Desarrollo histórico

La historia ha sido testigo de un buen número de sistemas de cifra. Entre ellos podemos destacar en orden cronológico los siguientes:

Siglo V a.C.: Escítala	Siglo II a.C.: Polybios	Siglo I a.C.: César	1467: Alberti
1508: Trithemius	1553: Battista	1586: Vigenère	1710: Beaufort
1821: Beale	1854: Playfair	1860: Wheatstone	1891: Bazeries
1917: Vernam	1923: Enigma	1927: Hagelin	1927: Hagelin

Figura 3.2. Algoritmos de cifra clásica más conocidos.

De estos sistemas, veremos en este capítulo el funcionamiento en operaciones de cifrado y descifrado, así como los ataques ante los cuales sucumben, del algoritmo del César y una variación conocida como cifrado Afín, del algoritmo de Vigenère y del algoritmo de Hill. Todos ellos algoritmos por sustitución. En cuanto la cifra por transposición, tuvo un recorrido muy corto en la criptografía clásica, siendo la escítala el sistema más conocido.

Dejando de lado a la máquina Enigma y otras similares, muy famosas por el papel desempeñado durante la Segunda Guerra Mundial, los cuatro algoritmos mencionados son los más representativos de dicho grupo de cifra por sustitución.

3. Clasificación de la cifra clásica

Los sistemas de criptografía clásica se clasifican de acuerdo al tipo de operación que se realizará al texto en claro durante la cifra, bien sea ésta la de transposición para lograr la difusión, o bien la de sustitución para lograr la confusión.

En la figura 3.3 se muestra un cuadro resumen de los principales sistemas de cifra clásica, según sean éstos de transposición o de sustitución.

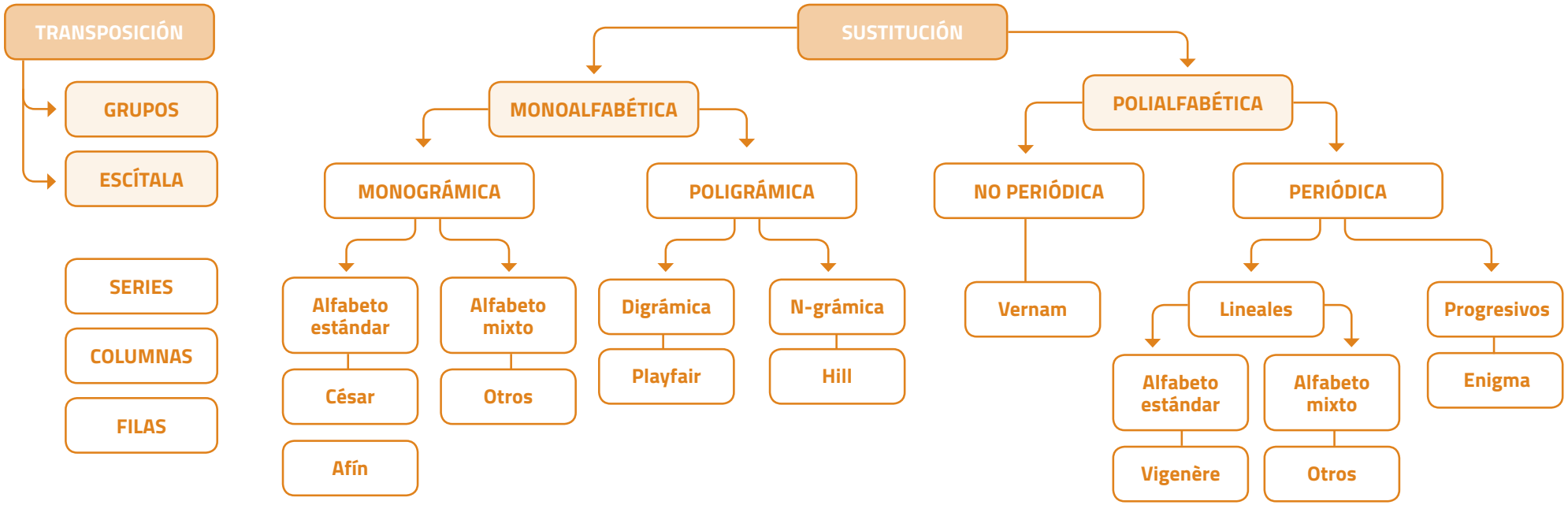


Figura 3.3. Clasificación de los sistemas de cifra clásica.

4. Algoritmos más conocidos de la cifra clásica

El algoritmo del César

El algoritmo del César es una cifra por sustitución monoalfabética (un único alfabeto de cifrado) y monográmica (se cifra letra a letra).

Es decir, se sustituye cada carácter del texto en claro por el carácter correspondiente de un único alfabeto de cifrado. En el caso del César, el alfabeto de cifrado se generaba mediante un desplazamiento constante de 3 espacios en alfabeto en claro de como se muestra en la figura 3.4.

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

Figura 3.4. Alfabeto de cifrado del César en módulo 27.

Si M es el texto en claro (letra a cifrar), b es el desplazamiento, n es el módulo de cifra (tamaño del alfabeto) y C es el criptograma resultante, las operaciones matemáticas del cifrado y del descifrado en un sistema del tipo César serán:

C = M + b mod n **César mod 27: C = M + 3 mod 27**

M = C - b mod n **César mod 27: M = C - 3 mod 27**

Por ejemplo, el cifrado mediante algoritmo del César del texto en claro ZOMBI y su posterior descifrado serán:

Código del mensaje ZOMBI según figura 4.1: 26; 15; 12; 1; 8.

Cifrado de la Z: 26 + 3 mod 27 = 30 mod 27 = 02 = C
Descifrado de la C: 02 – 3 mod 27 = -1 mod 27 = 26 = Z

Cifrado de la O: 15 + 3 mod 27 = 18 mod 27 = 18 = R
Descifrado de la R: 18 – 3 mod 27 = 15 mod 27 = 15 = O

Cifrado de la M: 12 + 3 mod 27 = 15 mod 27 = 15 = O
Descifrado de la O: 15 – 3 mod 27 = 12 mod 27 = 12 = M

Cifrado de la B: 1 + 3 mod 27 = 4 mod 27 = 4 = E
Descifrado de la E: 4 – 3 mod 27 = 1 mod 27 = 1 = B

Cifrado de la I: 8 + 3 mod 27 = 11 mod 27 = 11 = L
Descifrado de la L: 11 – 3 mod 27 = 8 mod 27 = 8 = I

C = CROEL
M = ZOMBI

El cifrado Afín

En el cifrado afín, primero se multiplica el código de la letra a cifrar por una constante a y posteriormente se aplica un desplazamiento de b espacios. Por lo tanto, en este caso las operaciones de cifrado y descifrado serán:

C = a*M + b mod n **M = (C – b) inv (a, n) mod n**

La figura 3.5 muestra el alfabeto de cifrado para la cifra afín M = 2*M + 4 mod 27.

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

Figura 3.5. Alfabeto de cifrado módulo 27 con decimación a = 2 y desplazamiento b = 4.

Por lo tanto, ahora el texto en claro ZOMBI se cifrará y descifrará en modo afín con a = 2 y b = 4 en módulo 27 de la siguiente manera:

Código del mensaje ZOMBI según figura 4.2: 26; 15; 12; 1; 8.
Además, sabemos que inv (2, 27) = 14.

Cifrado de la Z: 2*26 + 4 mod 27 = 56 mod 27 = 2 = C
Descifrado de la C: (2 – 4)*14 mod 27 = -28 mod 27 = 26 = Z

Cifrado de la O: 2*15 + 4 mod 27 = 34 mod 27 = 7 = H
Descifrado de la H: (7 – 4)*14 mod 27 = 42 mod 27 = 15 = O

Cifrado de la M: 2*12 + 4 mod 27 = 28 mod 27 = 1 = B
Descifrado de la B: (1 – 4)*14 mod 27 = -42 mod 27 = 12 = M

Cifrado de la B: 2*1 + 4 mod 27 = 6 mod 27 = 6 = G
Descifrado de la G: (6 – 4)*14 mod 27 = 28 mod 27 = 1 = B

Cifrado de la I: 2*8 + 4 mod 27 = 20 mod 27 = 20 = T
Descifrado de la T: (20 – 4)*14 mod 27 = 224 mod 27 = 8 = I

C = CHBGT
M = ZOMBI

El cifrado de Vigenère

Las cifras anteriores, César y Afín y otras similares, eran monoalfabéticas. Por lo tanto, su fortaleza será muy baja en tanto la redundancia del lenguaje se manifestará de manera clara en el criptograma como veremos en el siguiente apartado.

Varios siglos después, nacen los sistemas de cifra polialfabéticos; es decir, en los que existe más de un alfabeto de cifra, de manera que la misma letra del texto en claro (por ejemplo la E) se cifrará como diferentes letras del alfabeto de acuerdo a una clave. Por lo tanto, habrá más de un alfabeto de cifra y ello significará una mayor fortaleza del sistema de cifra porque la redundancia del lenguaje ya no se manifiesta de manera tan clara en el criptograma.

El sistema más conocido de cifra por sustitución polialfabética monográmica es el de Vigenère. En este sistema, el mensaje se va cifrando letra a letra con una clave o palabra o texto K que se repite de manera periódica durante el proceso, como se indica en las ecuaciones siguientes:

$$C = M + K \bmod n \qquad M = C - K \bmod n$$

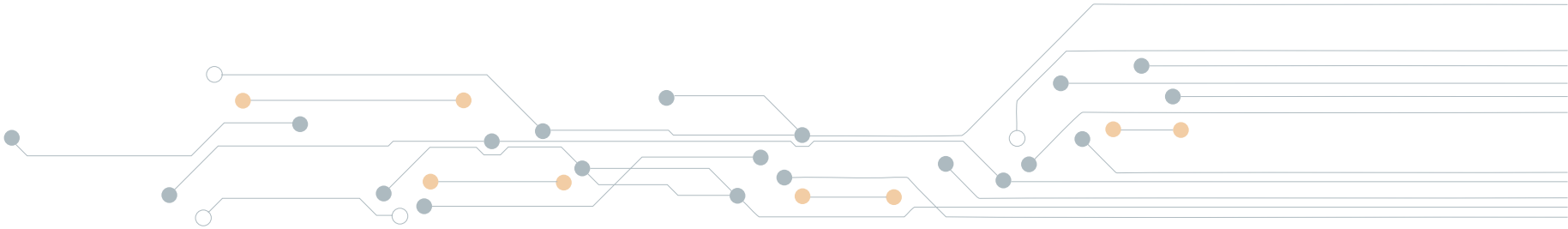
A continuación, se muestra cómo se cifraría el mensaje HERMOSO con la clave CIELO y su posterior descifrado.

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

Figura 3.6. Alfabeto en claro mod 27.

Texto en claro M	H = 7	E = 4	R = 18	M = 12	O = 15	S = 19	O = 15
Clave K	C = 2	I = 8	E = 4	L =11	O = 15	C = 2	I = 8
Suma	9	12	22	23	30	21	23
Reducción mod 27	9	12	22	23	3	21	23
Criptograma C	J	M	V	W	D	U	W

Tabla 3.1. Cifrado Vigenère del texto HERMOSO con la clave CIELO.



La cifra polialfabética destruye las relaciones directas que existía en la cifra monoalfabética entre el texto en claro y el criptograma. Así, en este caso la misma letra del texto en claro se cifrará de forma distinta en función de la letra de la clave con la que coincida durante la cifra y, por otra parte, dos letras iguales del criptograma podrán provenir de letras distintas en el texto en claro, dos cosas que no sucedían con la cifra monoalfabética.

Esta característica de la cifra polialfabética hace que si la clave K usada tiene más de 6 letras diferentes, las frecuencias de las letras en el criptograma se suavizan (las menos frecuentes aumentan y las más frecuentes disminuyen), de forma tal que ya no podremos asociar la letra más frecuente del criptograma con la letra más frecuente del texto en claro, aumentando por tanto la fortaleza del algoritmo ante el criptoanálisis basado en la redundancia del lenguaje.

La figura 3.7 muestra el efecto antes comentado. La letra O del texto en claro se cifra como la letra D o como la letra W, y la letra W del criptograma procede de la letra M y de la letra O del texto en claro.

H	E	R	M	O	S	O
C	I	E	L	O	C	I
J	M	V	W	D	U	W

H	E	R	M	O	S	O
C	I	E	L	O	C	I
J	M	V	W	D	U	W

Tabla 3.1. Cifrado Vigenère del texto HERMOSO con la clave CIELO.

El cifrado de Hill

El cifrado de Hill consiste en una cifra por sustitución monoalfabética n-grámica, es decir ciframos bloques de dos o más letras, de la misma manera que se hace en la actualidad en los sistemas de cifra modernos como el AES, si bien aquí se habla de bytes y no de letras.

Para ello, Hill usa una matriz cuadrada como clave, en función del n-grama utilizado. La operación de cifra será la multiplicación del mensaje en bloques de n-gramas por la matriz clave K y su posterior reducción módulo n, y el descifrado será la multiplicación del criptograma C en bloques de n-gramas por la clave K inversa en ese cuerpo de cifra y su posterior reducción módulo n.

Observa que en el descifrado su utiliza la matriz inversa de la clave K en módulo n; por lo tanto, la matriz clave utilizada para la cifra deberá tener inversa en el cuerpo de cifra. Para cumplir esta condición, será necesario que el máximo común denominador entre el determinante de K y el módulo n sea igual a la unidad, es decir: mcd (|K|, n) = 1.

La figura 3.8 muestra la cifra de del mensaje ZOMBI (26; 15; 12; 1; 8) mediante trigramas mod 27, usando la letra X = 24 como relleno.

Es decir, cifraremos dos trigramas: ZOM y BIX con códigos {26, 15, 12} y {1, 8, 24}.

Primer bloque

$$\begin{pmatrix} M_1 = 26 \\ M_2 = 15 \\ M_3 = 12 \end{pmatrix} \begin{pmatrix} K_{11} = 19 & K_{12} = 6 & K_{13} = 15 \\ K_{21} = 24 & K_{22} = 18 & K_{23} = 26 \\ K_{31} = 6 & K_{32} = 13 & K_{33} = 10 \end{pmatrix} \text{mod } 27 = \begin{pmatrix} C_1 = 8 \\ C_2 = 18 \\ C_3 = 12 \end{pmatrix}$$

Segundo bloque

$$\begin{pmatrix} M_1 = 1 \\ M_2 = 8 \\ M_3 = 24 \end{pmatrix} \begin{pmatrix} K_{11} = 19 & K_{12} = 6 & K_{13} = 15 \\ K_{21} = 24 & K_{22} = 18 & K_{23} = 26 \\ K_{31} = 6 & K_{32} = 13 & K_{33} = 10 \end{pmatrix} \text{mod } 27 = \begin{pmatrix} C_1 = 22 \\ C_2 = 9 \\ C_3 = 26 \end{pmatrix}$$

Figura 3.8. Cifrado de Hill trigrámico módulo 27.

Los bloques se cifran multiplicando la columna del mensaje por cada fila de la matriz clave, es decir:

Primer bloque:

(26x19 + 15x6 + 12x15) mod 27 = (494 + 90 + 180) mod 27 = 764 mod 27 = 8 = I

(26 x24 + 15x18 + 12x26) mod 27 = (624 + 270 + 312) mod 27 = 1.206 mod 27 = 18 = R

(26 x6 + 15x13 + 12x10) mod 27 = (156 + 195 + 120) mod 27 = 471 mod 27 = 12 = M

Segundo bloque:

(1x19 + 8x6 + 24x15) mod 27 = (19 + 48 + 360) mod 27 = 427 mod 27 = 22 = V

(1x24 + 8x18 + 24x26) mod 27 = (24 + 144 + 624) mod 27 = 792 mod 27 = 9 = J

(1x6 + 8x13 + 24x10) mod 27 = (6 + 104 + 240) mod 27 = 350 mod 27 = 26 = Z

El criptograma será C = [8, 18, 12], [22, 9, 26] = IRM VJZ

Para el descifrado del criptograma IRM VJZ habrá que utilizar la clave inversa de la matriz [K] como se muestra en la figura 3.9. Observa que la matriz inversa [K-1] no es igual que la directa [K]; de hecho debe cumplirse que [K-1] * [K] mod 27 = [I], la matriz identidad.

Primer bloque

$$\begin{pmatrix} C_1 = 8 \\ C_2 = 18 \\ C_3 = 12 \end{pmatrix} \begin{pmatrix} K_{11} = 19 & K_{12} = 0 & K_{13} = 12 \\ K_{21} = 6 & K_{22} = 16 & K_{23} = 25 \\ K_{31} = 24 & K_{32} = 17 & K_{33} = 9 \end{pmatrix} \text{ mod 27 = } \begin{pmatrix} C_1 = 26 \\ C_2 = 15 \\ C_3 = 12 \end{pmatrix}$$

Segundo bloque

$$\begin{pmatrix} M_1 = 22 \\ M_2 = 9 \\ M_3 = 26 \end{pmatrix} \begin{pmatrix} K_{11} = 19 & K_{12} = 0 & K_{13} = 12 \\ K_{21} = 6 & K_{22} = 16 & K_{23} = 25 \\ K_{31} = 24 & K_{32} = 17 & K_{33} = 9 \end{pmatrix} \text{ mod 27 = } \begin{pmatrix} C_1 = 1 \\ C_2 = 8 \\ C_3 = 24 \end{pmatrix}$$

Figura 3.9. Descifrado de Hill trigrámico módulo 27 con matriz clave inversa [K-1].

Los bloques se descifran multiplicando la columna del criptograma por cada fila de la matriz clave inversa, es decir:

Primer bloque:

(8x19 + 18x0 + 12x12) mod 27 = (152 + 0 + 144) mod 27 = 296 mod 27 = 26 = Z

(8x6 + 18x16 + 12x25) mod 27 = (48 + 288 + 300) mod 27 = 636 mod 27 = 15 = O

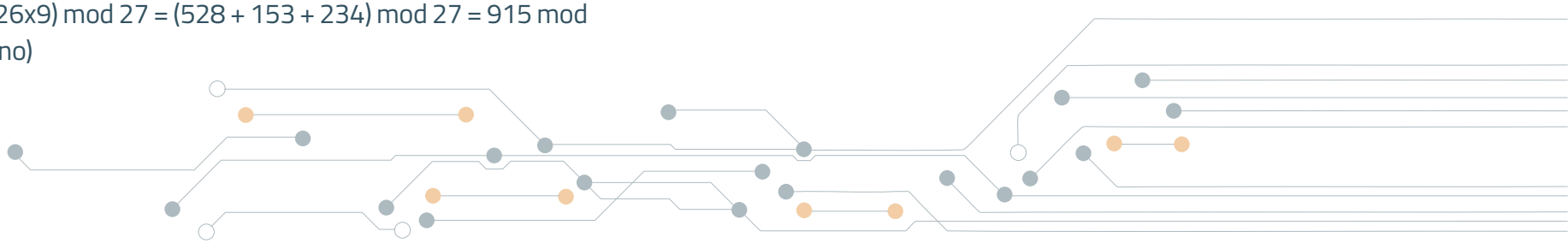
(8x24 + 18x17 + 12x9) mod 27 = (192 + 306 + 108) mod 27 = 606 mod 27 = 12 = M

Segundo bloque:

(22x19 + 9x0 + 26x12) mod 27 = (418 + 0 + 312) mod 27 = 730 mod 27 = 1 = B

(22x6 + 9x16 + 26x25) mod 27 = (132 + 144 + 650) mod 27 = 926 mod 27 = 8 = I

(22x24 + 9x17 + 26x9) mod 27 = (528 + 153 + 234) mod 27 = 915 mod 27 = 24 = X (relleno)



5. Criptoanálisis de los sistemas de cifra clásica

El cifrado con algoritmo del César es tan elemental, que es más eficiente realizar un ataque por fuerza bruta que un criptoanálisis, en tanto los únicos posibles desplazamientos en módulo 27 son 26. Así, provocando sucesivos desplazamientos a la izquierda o a la derecha, en el peor de los casos se dará con el texto en claro en la operación número 26.

Si se desea criptoanalizar el criptograma, basta con contabilizar las frecuencias con las que aparecen las letras en ese criptograma y asociar la letra a la letra más frecuente del criptograma con la letra más frecuente de un texto en claro, que para español o inglés debería ser la E. Si esto falla, podemos usar la A en vez de la E y en casos extremos la letra O. Esto es así porque son la letra E, la letra A y la letra O son las 3 letras más frecuentes en el castellano, como se observa en la figura 3.10.

Figura 3.10. Estadísticas típicas del lenguaje español en módulo 27.

Por ejemplo, si el criptograma fuese C = JXYJY JCYTJ XZRJÑ JQUPT HPFWT IJVZJ JRZRF HNKWF UTWXZ XYNYZ HNTRQ TRTFP KFGJY NHFPF XJXYF INXYN HFXIJ PPJRL ZFÑJX JQFRN KNJXY FRYFQ GNJRJ RJPHW NUYTL WFQF, y sabemos que se trata de una cifra por sustitución tipo César, pero no conocemos la constante de desplazamiento, contabilizamos la frecuencia de aparición de las letras y obtenemos:

J	F	X	Y	N	
19 veces	15 veces	10 veces	11 veces	10 veces	...
14,6%	11,5%	7,7%	8,4%	7,7%	

Si suponemos que la E se ha cifrado como J, entonces E + b mod 27 = J; es decir, 4 + b mod 27 = 9. Por lo tanto, b podría ser igual a 5. Para comprobar si es verdad, desciframos las primeras 15 letras del criptograma JXYJY JCYTJ XZRJÑ y obtenemos ESTET EXTOE SUNEJ. Está claro que se trata de texto en español. El texto en claro es: ESTE TEXTO ES UN EJEMPLO CLARO DE QUE EN UNA CIFRA POR SUSTITUCION MONOALFABETICA LAS ESTADISTICAS DEL LENGUAJE SE MANIFIESTAN TAMBIEN EN EL CRIPTOGRAMA.

La costumbre de formar bloques de 5 letras en el criptograma, proviene del uso de la telegrafía para enviar esos mensajes cifrados.

Si ahora la cifra es tipo Afín, habrá que plantear un par de ecuaciones independientes, asignando a la letra más frecuente del criptograma la cifra de la letra E del castellano (la más frecuente), y asignando a la segunda letra más frecuentes del criptograma la cifra de la letra A del castellano (la segunda más frecuente). Si el ataque no prospera, es posible que esas asignaciones hayan sido las contrarias y se hace este nuevo intento. Si seguimos sin dar con los valores de a y de b, podemos buscar otras asignaciones o bien incluir en este procedimiento a la letra O, la tercera más frecuente del castellano.

Sea el criptograma C = WCGWG WVGNW CKFWP WBQXN OXHYN SWUKW WFKFH OMAYH QNYCK CGMGK OMNFB NFNHX AHLWG MOHXH CWCGH SMCGM OHCSW XXWFE KHPWC WBHFM AMWCG HFGHB LMWFW FWXOY MQGNE YHBH, resultado de una cifra afín. Los caracteres más frecuentes del criptograma son la W con un 14,7% y la H con un 11,6%. Actuando en consecuencia:

W = a*E + b mod 27

H = a*A + b mop 27 (como A = 0, b = H = 7

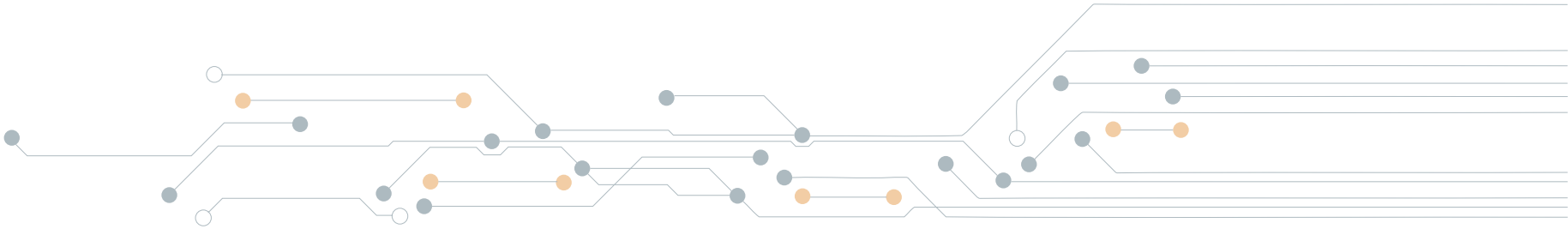
Como W = 23 y E = 4, reemplazando b = 7 en la primera ecuación, se obtiene:

23 = a*4 + 7 mod 27

A = (23 – 7) inv (4, 27) mod 27 = 16 * 7 mod 27 = 112mod 27 = 4

Como a = 4 es un valor válido porque mcd (4, 27) =1, probamos a ver si las claves eran a = 4 y b = 7, obteniendo:

M = ESTE TEXTO ES UN EJEMPLO CLARO DE QUE EN UNA CIFRA POR SUSTITUCION MONOALFABETICA LAS ESTADISTICAS DEL LENGUAJE SE MANIFIESTAN TAMBIEN EN EL CRIPTOGRAMA.



Cuando la cifra es polialfabética, como en el caso de Vigenère, este tipo de ataque ya no prospera porque las letras del texto en claro se cifran con los diferentes alfabetos que componen una clave y, por tanto, el efecto final es que las frecuencias de las letras en el criptograma tienden a ser todas muy similares, como ya se ha comentado, mostrando una distribución uniforme discreta.

Aquí la técnica de ataque se basa en el método de Kasiski, que se realiza en las siguientes fases:

1. Buscamos cadenas de caracteres de al menos 3 letras repetidas en el criptograma.

2. Encontramos la separación que hay entre las cadenas iguales y calculamos el máximo común divisor de todas esas separaciones. Este número nos dará la posible longitud de la clave, pero no las letras que la forman.

3. Si la clave tiene una longitud L, entonces habrá L subcriptogramas que se han cifrado con una misma letra, es decir todas son cifras monoalfabéticas.

4. Para encontrar las letras de la clave dividimos el criptograma en tantos subcriptogramas como sea esa longitud L encontrada.

5. Como cada uno de estos subcriptogramas será el resultado de una cifra monoalfabética, contabilizamos las veces que aparecen las letras en ellos y marcamos las 4 de mayor frecuencia.

6. Si estas letras más frecuentes guardan la misma separación que en el texto en claro tienen la A, la E, la O y la S, entonces como es lógico deberían corresponder a la cifra de las letras A, E, O y S.

7. Recuerda que en módulo 27 de la letra A (0) a letra la E (4) hay 4 espacios; de la letra E (4) a la letra O (15) hay 11 espacios; de la letra O (15) a la letra S (19) hay también 4 espacios; y de la letra S (19) a la letra A (0) hay 8 espacios.

8. La posición relativa que ocupa la letra A del texto en claro en ese subcriptograma, será la letra de la clave que buscamos.

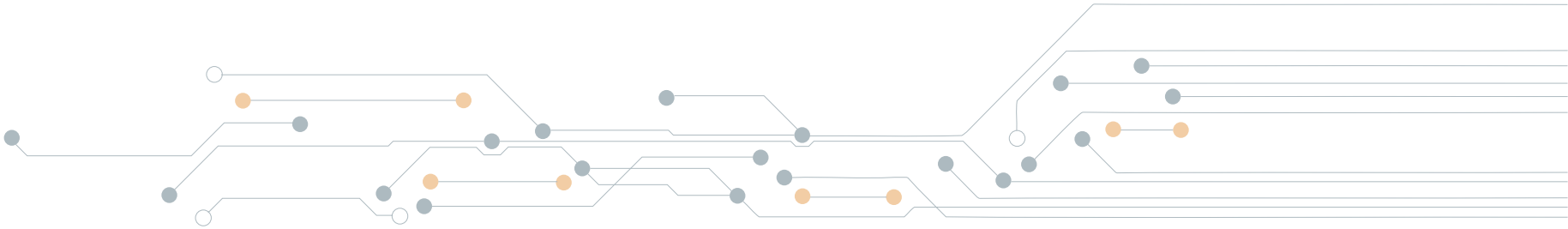


Figura 3.11. Ataque de Kasiski que encuentra la clave K = NEGRO.

El texto en claro corresponde al comienzo de la novela El gato negro, de Edgard Allan Poe: "No espero ni remotamente que se conceda el menor crédito a la extraña, aunque familiar historia que voy a relatar. Sería verdaderamente insensato esperarlo cuando mis mismos sentidos rechazan su propio testimonio. No obstante, yo no estoy loco, y ciertamente no sueño. Pero, por si muero mañana, quiero aliviar hoy mi alma."

Por último, en la cifra por matrices de Hill, como en el criptograma se destruyen todas las estadísticas del lenguaje, este tipo de ataque no es posible. Sin embargo, el algoritmo de Hill sucumbe fácilmente ante un ataque por texto en claro conocido. Al trabajar con matrices, se busca la matriz identidad mediante un proceso de Gauss-Jordan, y con muy poco texto en claro es posible encontrar la matriz clave.

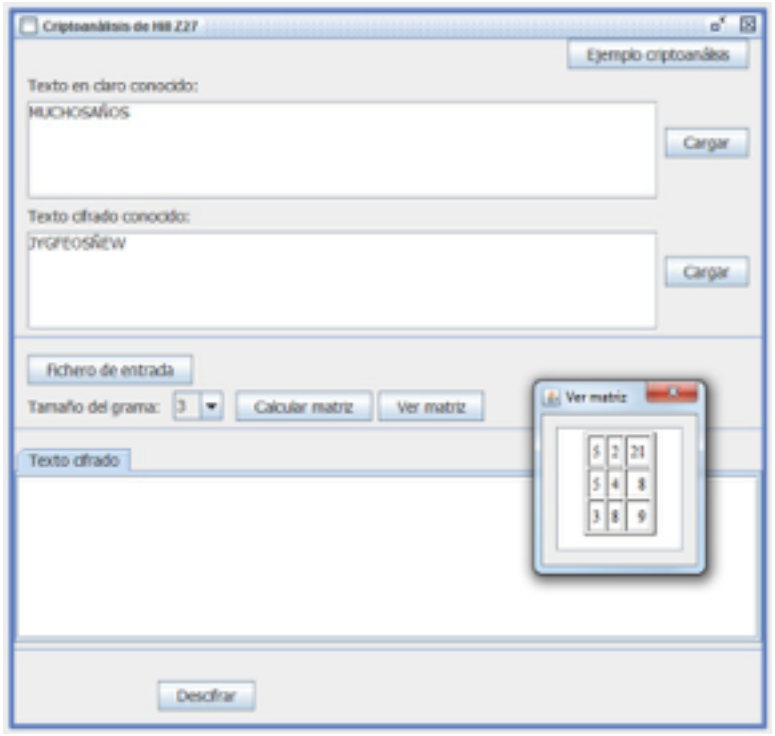


Figura 3.12. Ataque mediante Gauss-Jordan a una cifra de Hill trigrámica.

Por ejemplo si se cifra con la matriz clave trigrámica K = [5, 2, 21 - 5, 4, 8 - 3, 8, 9] el texto en claro M = Muchos años después, frente al pelotón de fusilamiento, se obtiene el criptograma C = JYG FEO SÑE WEJ BDW BBT TUÑ AIL JPI SFJ CPÑ MSY RZE DEG HPZ YJB, con letra Z como relleno. Para el criptoanálisis sólo nos hará falta tener los 10 primeros caracteres de las dos palabras "Muchos años" del inicio del texto en claro y los correspondientes 10 primeros caracteres del criptograma, es decir C = JYG FEO SÑE W. La figura 3.12 muestra cómo usando el software Criptoclásicos V2.1, se encuentra la matriz clave con muy poco texto en claro conocido.

Telefónica EDUCACIÓN DIGITAL