LA CRIPTOGRAFÍA CLÁSICA

Santiago Fernández (*)

En la Universidad de Yale se encuentra un manuscrito de 235 páginas, donado, en 1969, por H.P Kraus. El manuscrito, adquirido por Wilfrid M. Voynich en 1912, pertenecía a un colegio jesuita situado en Villa Mondragone, cerca de Roma. Escrito por un autor desconocido (aunque algunos lo atribuyen a **Roger Bacon**, uno de los grandes personajes del S.XIII), constituye en sí mismo todo un enigma, ya que está escrito con unos caracteres extraños, y que hasta la fecha nadie ha logrado descifrar. Se conoce como el *El manuscrito Voynich*. Es sin duda uno de los grandes retos del desciframiento.

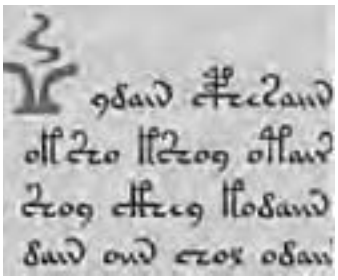


Figura 1. Un trozo de página del *manuscrito Voynich*

1. ESTEGANOGRAFÍA Y CRIPTOGRAFÍA

La comunicación secreta lograda mediante la ocultación de la existencia de un mensaje se conoce con el nombre de **esteganografía**, derivado de las palabras στεγανο(steganpos), que significa encubierto, y γραπτοζ (gráphos), que significa escritura.

En el siglo V a.C. el gran historiador griego **Herodoto** describió la manera que tenían los griegos para mandarse mensajes entre sí. El procedimiento básicamente consistía en escribir el mensaje sobre una tablilla de madera para posteriormente ocultarle mediante un recubrimiento de cera. El mismo Herodoto narra la historia de Histaiaeo en la cual se afeita la cabeza a un mensajero para luego escribir el mensaje sobre su cuero cabelludo y posteriormente esperar a que le crezca el pelo, antes de remitir el mensaje a la persona deseada; de ésta manera el mensajero pudo viajar hasta su destino sin ser molestado, al afeitarse su cabeza fue capaz de mostrar al receptor el mensaje oculto.

También, en la antigua civilización china se escribían mensajes sobre seda fina, que luego era aplastada hasta formar una pelotita que a su vez era recubierta de cera. En el siglo XV, el científico italiano **Gioavanni Porta** describe con todo lujo de detalles la manera de esconder un mensaje dentro de un huevo cocido. La esteganografía incluye también la práctica de escribir con tinta invisible, procedimiento ampliamente estudiado por casi todas las culturas.

Durante la segunda guerra mundial el sistema más utilizado consistió en microfilmar un mensaje y reducirlo hasta el extremo de un pequeño punto, de forma que podía pasar como un signo de puntuación de un carácter dentro de otro texto. Por ejemplo, el punto de consonante "j" podía ser en realidad un microfilm con un mensaje.

(*) Asesor de matemáticas del Berritzegune de Abando (Bilbao).

Con la llegada de los ordenadores se han ampliado y diversificado las técnicas esteganográficas. Una de las más comunes consiste en esconder un mensaje dentro de contenidos multimedia, mezclando los bits del mensaje original entre los bits del archivo gráfico o de sonido. El archivo resultante será una imagen o archivo de audio totalmente funcional que, a primera vista, no levanta ninguna sospecha, pero con el software adecuado es posible extraer la información oculta.

Actualmente, un grupo de investigadores de la Universidad George Mason, de Virginia, trabajan desde hace años en una herramienta capaz de detectar imágenes "esteganografiadas" en Internet. La novedosa ciencia, denominada **esteganálisis**, permite detectar información escondida en imágenes o archivos de sonido.

Pero, por muy bien que ocultemos los mensajes corremos el riesgo que tras una revisión concienzuda alguien sea capaz de descubrirlos, lo que claramente compromete la seguridad. Por esta razón la ocultación física de los mensajes ha dejado paso, a otro procedimiento más sofisticado: **La criptografía.**

El objetivo de la criptografía no es ocultar la existencia de un mensaje, sino más bien ocultar su significado, un proceso que se conoce como codificación.

2. LA CRIPTOLOGÍA

La criptología[1] (del griego krypto y logos, significa el estudio de lo oculto, lo escondido) es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones (en términos informáticos, ese canal suele ser una red de computadoras).

Esta ciencia está dividida en dos grandes ramas: **la criptografía**, ocupada del cifrado de mensajes en clave y del diseño de criptosistemas, y el **criptoanálisis**, que trata de descifrar los mensajes en clave, rompiendo así el criptosistema.

La **criptografía** es la disciplina que se encarga del estudio de códigos secretos o llamados también códigos cifrados (en griego *kriptos* significa secreto y *gráhos*, escritura).

La criptografía es una disciplina muy antigua, sus orígenes se remontan al nacimiento de nuestra civilización. En origen, su único objetivo era el proteger la confidencialidad de informaciones militares y políticas. Sin embargo, en la actualidad es una ciencia interesante no sólo en esos campos, sino para cualquier otro que esté interesado en la confidencialidad de unos determinados datos.

Aunque el objetivo original de la criptografía era mantener en secreto un mensaje, en la actualidad no se persigue únicamente **la privacidad o confidencialidad** de los datos, sino que se busca además garantizar la **autenticación** de los mismos (el emisor del mensaje es quien dice ser, y no otro), **su integridad** (el mensaje que leemos es el mismo que nos enviaron) y **su no repudio** (el emisor no puede negar el haber enviado el mensaje).

3. BREVE HISTORIA DE LA CRIPTOGRAFÍA

3.1. La Criptografía antigua

Cuestiones militares, religiosas y comerciales impulsaron desde tiempos remotos el uso de escrituras secretas. Ya los antiguos egipcios usaron métodos criptográficos. Por ejemplo, **los**

sacerdotes egipcios utilizaron la escritura hierática (jeroglífica) que era claramente incomprensible para el resto de la población. Los **antiguos babilonios** también utilizaron métodos criptográficos en su escritura cuneiforme.

Figura 2: Criptogramas egipcios
(a la izquierda, textos "en clave", con los textos "descifrados" a la derecha)

3.1.1. La escitala espartana

El primer caso claro de uso de métodos criptográficos se dio durante la guerra entre Atenas y Esparta. El historiador griego Plutarco, describe *la escitala* de la siguiente manera:

> "La escitala era un palo o bastón en el cual se enrollaba en espiral una tira de cuero. Sobre esa tira se escribía el mensaje en columnas paralelas al eje del palo. La tira desenrollada mostraba un texto sin relación aparente con el texto inicial, pero que podía leerse volviendo a enrollar la tira sobre un palo del mismo diámetro que el primero".

Con este sistema los gobernantes de Espartana transmitieron, con eficacia, sus instrucciones secretas a los generales de su ejército, durante las campañas militares.

Lógicamente, este procedimiento suponía que tanto el emisor como el receptor del mensaje dispusieran de un palo o bastón con las mismas características físicas: grosor y longitud.

Ejemplo:

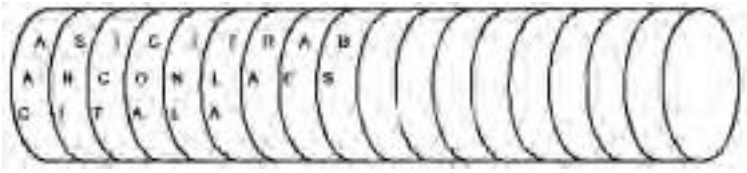


Figura 3. La escitala espartana

El texto a remitir es : ASI CIFRABAN CON LA ESCITALA, mientras que el texto cifrado o criptograma será: AAC SNI ICT COA INL FLA RA AE BS

3.1.2. El Cifrario de César

Este método fue empleado en los tiempos de la Roma Imperial. El algoritmo de César, llamado así porque es el procedimiento que empleaba **Julio César** para enviar mensajes secretos a sus legiones, es uno de los algoritmos criptográficos más simples. Es un algoritmo de **sustitución**, su cifrado consistía simplemente en sustituir una letra por la situada tres lugares más allá en el alfabeto esto es la A se transformaba en D, la B en E y así sucesivamente hasta que la Z se convertía en C.

Alfabeto 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
Alfabeto 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

Por ejemplo : El mensaje **FIRMA LA PAZ** se convierte en **ILUPD OD SDC**

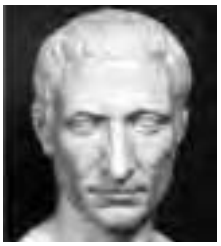


Figura 4. Julio César

Nota: Hoy en día, cualquier alfabeto que esté codificado con el alfabeto desplazado pero en su orden se llama "cifrado de César", aun cuando la letra inicial sea diferente de la D:

Tratamiento matemático:

Si asignamos a cada letra un número (A =00, B =01, C=02,.....Z=25), y consideramos un alfabeto de 26 letras, la transformación criptográfica en términos matemáticos se puede explicar bajo la siguiente fórmula de congruencias:

$C \equiv (M + 3)$ (mód 26)
M, corresponde a la letra del mensaje original
C, es la letra correspondiente a M pero en el mensaje cifrado.

Obsérvese que este algoritmo ni siquiera posee clave, puesto que la transformación siempre es la misma. Obviamente, para descifrar basta con restar 3 al número de orden de las letras del criptograma.

Ejemplo:

Asumiendo un alfabeto de 26 símbolos como el siguiente:

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

vamos a cifrar el siguiente mensaje: **PAZ**

Podemos hacerlo manualmente o utilizado la fórmula anteriormente dada:

1. Reemplazar **M** por el valor de la primera letra, en este caso P equivale a 15.
2. Realizar la operación indicada: **C = (15 + 3) (mód 26) = 18.**
3. Corresponder el número obtenido con la letra , en nuestro caso la S.
4. Realizar la operación con las letras restantes.

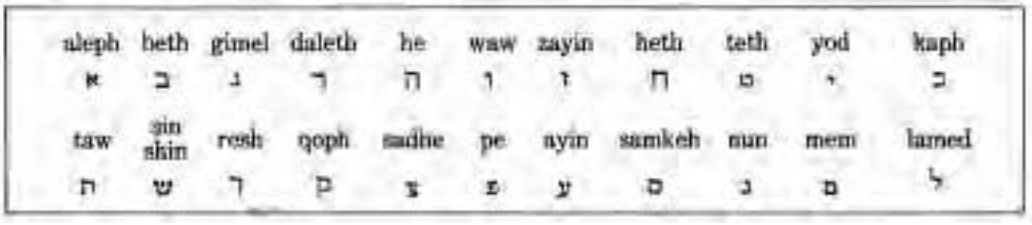
Así obtenemos las siguientes correspondencias :

M	**C**
P	S
A	D
Z	C

Por tanto el Mensaje Codificado es : **SDC** (la palabra **PAZ** se ha convertido en **SDC**).

3.1.3. El atbash hebreo

El atbash se emplea en el libro de Jeremías.25,26 de la Biblia, donde la palabra Babilonia, en hebreo: *Babel* se convierte en *Sheshash*. Las letras del mensaje de origen se sustituyen una a una, de acuerdo con la norma siguiente: si la letra original se encuentra en la línea superior se sustituye por la letra correspondiente de la línea inferior, y a la inversa. De esta manera la a (aleph) se convierte en t (aw), y la letra b(eth) se convierte en sh(in). Por tanto la palabra Babel se convierte en Sheshash.



En nuestro alfabeto el procedimiento que usa el *atbash* es el siguiente:

1. Se disponen las letras del alfabeto original de izquierda a derecha, desde la a hasta a la m; luego se continua la serie, de derecha a izquierda, de la n a la z, pero dispuestas en una hilera paralela a la anterior, y que van a corresponder a las letras del alfabeto cifrado.

Alfabeto[(1)] original	a	b	c	d	e	f	g	h	i	j	k	l	m
Alfabeto Cifrado	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

2. Se realiza la misma operación con las letras restantes.

Alfabeto original	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto Cifrado	M	L	K	J	I	H	G	F	E	D	C	B	A

3. Por último para cifrar, se hace corresponder la letra superior con su correspondiente inferior, siendo esta última la que figura en el texto cifrado.

Veamos un ejemplo:

El mensaje **firma la paz** se convierte en **URINZ AZ KZA**

El procedimiento usado es de tipo **monoalfabético**.

3.1.4. El método de Polybios

El escritor griego Polybios, inventó un sistema que acabó siendo adoptado muy a menudo como método criptográfico. Colocó las letras del alfabeto en una red cuadrada de 5x5. El sistema de cifrado consistía en hacer corresponder a cada letra del alfabeto un par de letras que indicaban la fila y la columna , en la cual aquella se encontraba.

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

Tablero de Polibio

Así por ejemplo el texto: **deseamos la paz**
se convertía en: **ADAEDCAEAACBCDDC CAAA CEAAEE**

Si en el tablero de Polybios introducimos números, resulta una variante sumamente interesante:

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

Cada letra viene representada por dos números, el de su fila y el de su columna.
Así, K = 25, w = 5, mientras que la letras N y Ñ tienen una misma representación, en nuestro caso el 33. El mensaje anterior, de acuerdo a esta codificación numérica se traduce en:

1415431511323443 3111 351155

Polybios sugería usar este sistema como método de transmisión de mensajes a larga distancia (usando antorchas o fogatas, por ejemplo). Pero, sin duda, el gran éxito de su método reside en la conversión de letras en números, la reducción en el número de caracteres finales, y la división de una unidad en dos partes manipulables separadamente. Lo que ha servido de base para otros sistemas de cifrado, es el caso del sistema Playfair.

Los cuatro sistemas ilustran dos de los principios esenciales en los que se basa la criptografía clásica: ***la sustitución y la transposición.***

El Cifrario de César, El atbash hebreo y el sistema de Polybios son ejemplos de ***sustitución*** *(cada una de las letras del mensaje original tiene una correspondencia fija en el mensaje cifrado).*

Mientras que la escítala espartana es un ejemplo de ***transposición*** *(las letras simplemente se cambian de sitio o se transponen, por tanto las letras son las mismas en el mensaje original y en el cifrado. En términos de pasatiempos se dice que las letras se trasponen o se* ***anagraman****).*

En principio, parece muy difícil descubrir el mensaje cifrado por cualquiera de estos tres procedimientos, pero una persona inteligente y observadora puede descifrar el secreto sin demasiada dificultad. De hecho, estos sistemas se encuadran en una categoría de cifrarios que reciben el nombre de **degenerativos**.

3.2. La Criptografía medieval

Durante siglos la criptografía caminó por la senda de la sustitución y la transposición. En los escritos medievales sorprenden términos como Oobice o Thfpflxctxs. Para esconder sus nombres, los copistas empleaban el alfabeto zodiacal, formaban anagramas alterando el orden de las letras (es el caso de oobice, anagrama de Boecio) o recurrían a un método denominado fuga de vocales, en el que éstas se sustituían por puntos o por consonantes arbitrarias (Thfpflxctxs por Theoflactus).

Esta simplicidad hizo que la **sustitución** fuera el procedimiento dominante a lo largo del primer milenio de nuestra era. Por esa época, muchos estudiosos consideraban a la cifra de sustitución como indescifrable.

Sin embargo, en la ciudad de Bagdad se produjo el milagro del desciframiento. El artífice fue el sabio árabe Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi (801-873), más conocido como **Al-Kindi**, él fue un importante filósofo árabe y un estudioso de las Ciencias. Autor de unos 300 libros sobre: medicina, matemáticas, lingüística, música....Pero, uno de sus tratados más importantes, redescubierto el año 1987, en el archivo Sulaimaniyyah de Estambul, titulado: "Sobre el desciframiento de mensajes criptográficos".

El sistema para resolver los enigmas criptográficos está descrito claramente en dos breves párrafos, dice Al Kindi :

> "Una manera de resolver un mensaje cifrado, si sabemos en qué lengua está escrito, es encontrar un texto llano escrito en la misma lengua, suficientemente largo, y luego contar cuantas veces aparece cada letra. A letra que aparece con más frecuencia la llamamos "primera", a la siguiente en frecuencia la llamaremos"segunda"....y así hasta que hayamos cubierto todas las letras que aparecen en nuestro texto.
>
> Luego observamos el texto cifrado que queremos resolver y clasificamos sus símbolos de la misma manera. Encontramos el símbolo que aparece con mayor frecuencia y lo sustituimos por la "primera" de la nuestro texto, hacemos lo mismo con la "segunda" y así sucesivamente, hasta que hayamos cubierto todos los símbolos del criptograma que queremos resolver". (Al Kindi [3]).

Para facilitar el desciframiento siguiendo este procedimiento nos puede ayudar el saber cuales son las frecuencias relativas de las letras y de algunas palabras más frecuentes.

En lengua inglesa

Letra	Porcentaje	Letra	Porcentaje
a	8,2	n	6,7
b	1,5	o	7,5
c	2,8	p	1,9
d	4,3	q	0,1
e	12,7	r	6,0
f	2,2	s	6,3
g	2,0	t	9,1
h	6,1	u	2,8
i	7,0	v	1,0
j	0,2	w	2,4
k	0,8	x	0,2
l	4,0	y	2,0
m	2,4	z	0,1

Frecuencia de las letras en Inglés

Letras de alta frecuencia		Letras de frecuencia media		Letras de frecuencia baja	
Letra	Frecuencia %	Letra	Frecuencia %	Letra	Frecuencia %
e	12,7	d	4,3	b	1,5
t	9,1	l	4,0	v	1,0
a	8,2	c	2,8	k	0,8
o	7,5	u	2,8	El resto de las letras: j,q,x,z tienen frecuencias inferiores a 0.5% y se pueden considerar por tanto "raras":	
i	7,0	m	2,4		
n	6,7	w	2,4		
s	6,3	f	2,2		
h	6,1	g	2,0		
r	6,0	y	2,0		
	p	1,9			

En castellano haciendo un estudio similar tenemos:

Frecuencia de las letras en el castellano

Letras de alta frecuencia		Letras de frecuencia media		Letras de frecuencia baja	
Letra	Frecuencia %	Letra	Frecuencia %	Letra	Frecuencia %
e	16,78	r	4,94	y	1,54
a	11,96	u	4,80	q	1,53
o	8,69	i	4,15	b	0,92
l	8,37	t	3,31	h	0,89
s	7,88	c	2,92	El resto de las letras: g,f,v,w,j,z,x,k tienen frecuencias inferiores a 0.5% y se pueden considerar por tanto "raras":	
n	7,01	p	2,76		
d	6,87	m	2,12		

Frecuencia de las palabras en el castellano

Palabras más frecuentes		Palabras de dos letras		Palabras de tres letras		Palabras de cuatro letras	
Palabra	Frecuencia (por diezmil)	Palabra	Frecuencia (por diezmil)	Palabra	Frecuencia (por diezmil)	Palabra	Frecuencia (por diezmil)
de	778	de	778	que	289	para	67
la	460	la	460	los	196	como	36
el	339	el	339	del	156	ayer	25
en	302	en	302	las	114	este	23
que	289	se	119	por	110	pero	18
y	226	un	98	con	82	esta	17
a	213	no	74	una	78	años	14
los	196	su	64	mas	36	todo	11
del	156	al	63	sus	27	sido	11
se	119	es	47	han	19	solo	10
las	114						

En resumen, en un texto escrito en castellano, se pueden sacar las siguientes conclusiones (por término medio).

- Las vocales ocuparán alrededor del 47% del texto.
- Sólo la **e** y la **a** se identifican con relativa fiabilidad porque destacan mucho sobre las demás. De hecho, entre las dos vocales ocupan el 25% del mensaje.
- Las letras de frecuencia alta suponen un 68% del total.
- Las consonantes más frecuentes: **l, s, n, d** (alrededor del 30%).
- Las seis letras menos frecuentes: **v, ñ, j, z, x** y **k** (poco más del 1%).
- Las palabras más frecuentes **(de, la, el, en, ...)** que ocuparán el 30% del texto.

En el famoso relato el *escarabajo de oro*, escrito por el americano **Edgar Allan Poe** y publicado el año 1843, se describe como el héroe del relato, William Legrand, consigue descubrir el lugar en el que se encuentra un fabuloso tesoro, descifrando un mensaje criptográfico escrito sobre un pergamino. El procedimiento utilizado por W. Legrand para desentrañar el cifrario del pergamino es un método estadístico, basado en la frecuencia de las letras que componen un texto inglés. En definitiva,el método coincide exactamente con el propuesto por el sabio árabe **Al-Kindi**.

Hemos de reconocer que Poe era un excelente criptoanalista aficionado. También el escritor francés Julio Verne (1828-1905) utilizó la criptografía en varias de sus novelas, una de ellas *Viaje al centro de la Tierra*.

3.3 La Criptografía europea hasta el Renacimiento

3.3.1. Los precursores europeos

El primer libro europeo que describe el uso de la criptografía fue escrito en el siglo XIII por el monje franciscano **Roger Bacon**, su título es: *La Epístola sobre las obras de arte secretas y la nulidad de la magia*, en él se describen siete métodos distintos para mantener en secreto los mensajes.

Figura 6. Roger Bacon (1211-1292)

En esa época, las personas que se dedicaban a la criptografía eran conscientes de que los simples análisis de frecuencia hacían vulnerable sus cifrados. Por esta razón utilizaron dos trucos para luchar contra el análisis estadístico: los **homófonos** y las **nulas**.

- Los cifrados homofónicos consisten en trabajar con alfabetos más ricos que el normal (de 26 letras). Para ello se añaden algunas letras nuevas (♦♥♣♠), que corresponden a las letras de más alta frecuencia.

Por ejemplo:

Alfabeto original	a	a	b	c	d	e	e	f	g	h	i	i	j	k	l	m	n	o	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	G	V	♦	X	C	♥	F	P	A	W	K	B	N	E	♣	M	L	Z	S	T	Q	♠	I	D	Y	O	R	J	U	H

Podemos observar que se han repetido las vocales a,e,i,o y se han cifrado por mediante dos homófonos. Así los homófonos correspondientes a la A son, la G y la V, los homófonos correspondientes a la E son la ♥ y la F, y así sucesivamente. De esta manera el mensaje:

el río esta limpio se convierte en: F♣ ♠KZ FIDG ♣BMTKS

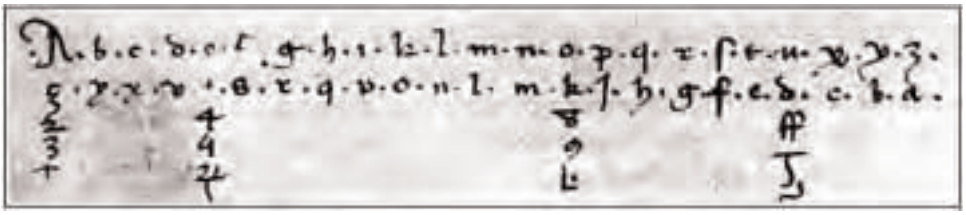


Figura 7. Sustitución homofónica de Simone de Crema, 1401

- Mientras que en los cifrados empleando nulos el objetivo es incluir en el mensaje de origen algunas letras carentes de significado y que naturalmente no interfieran en su comprensión.

Por ejemplo:

Cifrar el siguiente mensaje: **lla pazz no hha sidto ffirdmadoa**, cuando el mensaje llegue a su destino el descifrador no tiene problemas para recuperar el mensaje original: LA PAZ NO HA SIDO FIRMADA.

En este tipo de ciframientos conviene utilizar como nulas letras de baja frecuencia para alterar el análisis estadístico frecuencial.

En el siglo XIV el poeta y novelista ingl **Geoffrey Chaucer** también dedicó buena parte de su vida a estudiar la criptografía.

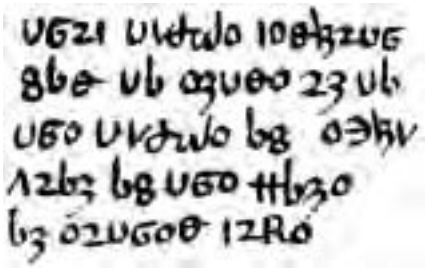


Figura 8. Mensaje criptográfico de G. Chaucer

El libro más antiguo del que se tiene constancia, y que trata enteramente sobre criptografía, es el *Liber Zifrorum* escrito por **Cicco Simoneta**, secretario de la Cancillería de los Sforza de Milán. El libro vio la luz el año 1474. Entre las personas que se dedicaron a la criptografía no podemos olvidar a **Giovanni Soro**, nombrado secretario de cifras en Venecia el año 1506.

En la mayoría de los casos la criptografía, en esta época, se refería exclusivamente a cifrarios **monoalfabéticos**. En ellos la sustitución clave, una vez elegida, no se modifica a lo largo de toda la operación de cifrado. Naturalmente podrían ponerse en correspondencia **alfabetos cifrantes** totalmente caóticos, lo que claramente dificultaría el posible desciframiento.

Ejemplo:

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

Por esa misma época también estuvo de moda el cifrado mediante dos o más alfabetos, alternando entre ellos, confundiendo de esta manera a los potenciales criptoanalistas(este es un salto cualtitativo ya que se pasa de cifrarios monoalfabéticos a cifrarios **polialfabéticos**[3] En esta línea hay que destacar a **León Battista Alberti** (1402-1472) que es considerado por muchos el abuelo de la criptología.

Veamos con un ejemplo como Alberti era capaz de cifrar los mensajes.

Alfabeto 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	iz
Alfabeto cifrado1	F	R	J	O	Y	D	I	Q	T	Z	S	L	M	E	U	N	B	K	W	A	H	P	C	X	G	V
Alfabeto cifrado2	H	T	R	V	Z	D	I	Q	J	Y	P	E	L	M	U	B	N	K	A	W	F	S	X	C	G	O

Para realizar el mensaje: **la ballesta**, se procedía de la siguiente manera:

La primera letra l, se convierte en M (del alfabeto1); a, se convierte en H(del alfabeto2); b, se convierte en R(del alfabeto 1); a, se convierte en H (del alfabeto2), y así se van alternando.... De manera que la palabra cifrada es: **MHRHLEYAAH**

Una ventaja evidente de este procedimiento es que una misma letra puede cifrarse de dos formas distintas, de acuerdo a la paridad del mensaje. Sin embargo, tiene la desventaja que es necesario conocer la disposición de dos alfabetos cifrados.

Con ánimo de mecanizar el cifrado, Alberti crea la primera máquina de criptografiar que consiste en dos discos concéntricos que giran independientes, consiguiendo con cada giro un alfabeto de transposición.

J. Trithemius

Si bien en el año 1470, León Battista Alberti publicó su Tratado de cifras, donde se describe una cifra capaz de encriptar un pequeño código. Se considera al abate **Johannes Trithemius** como padre de la criptografía moderna. Este religioso escribió en 1530 *Poligrafía*, el primer libro impreso sobre el tema. Trithemius introdujo el concepto de tabla ajustada, en el cual el alfabeto normal es permutado para codificar los mensajes.

León B. Alberti

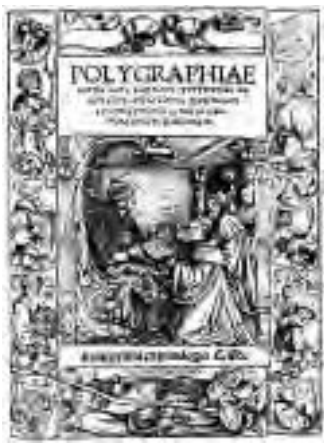


Figura 11. 1530 Poligrafía

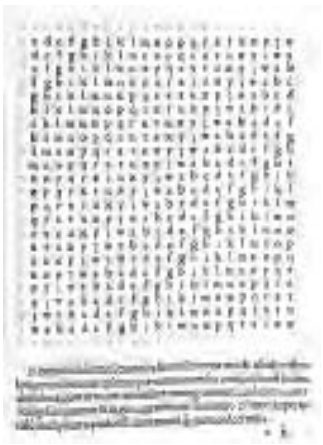


Figura 12. Una de las páginas del libro Poligrafía

Con la idea de reforzar la cifra de sustitución monoalfabética se introdujeron los **códigos**[5]. La idea es sustituir una palabra o varias por un determinado código o símbolo.

Por ejemplo:

Flandes = ⊕	Rey de Francia = ⊗	Reina de Inglaterra =	
Río Sena = ϰ	Reina de Escocia = Φ	Almirante = ϑ	Capturar =13
Matar = 34	hoy = 45	mañana = 56	atravesar = WD

El texto llano = **capturar al rey de Francia y atravesar el Sena**

Se convierte en el mensaje codificado:

Mensaje codificado: **13-⊗-WD-ϰ**

Puede parecer que los códigos son más seguros que las cifras, sin embargo para codificar mediante códigos es imprescindible redactar un libro de códigos, que seguramente tendría cientos de páginas. Además, dicho libro debería ser distribuido a todos los implicados (embajadores, militares, ..). Naturalmente si el libro cae en manos poco amigables el desastre sería total. Por ese motivo los criptógrafos comprendieron la dificultad del cifrado mediante códigos y confiaron sus mensajes a un sistema híbrido de cifras y de nomencladores[6].

3.4. Criptografia europea. Desde el Renacimiento hasta la Segunda Guerra Mundial

3.4.1. Blaise Vigenère

El francés Blaise de Vigenère, en el siglo XVI, desarrolló la teoría de la criptología polialfabética, por esta razón su nombre ha acabado asociado con uno de los métodos famosos de sustitución polialfabética. Lo que hoy se denomina "tablero de Vigenère" consiste en una disposición de letras que contiene en orden los 26 alfabetos de César. Además, para proteger más el cifrado suele introducirse una palabra **clave**, que consiste en una palabra o texto que se repite a largo de todo el mensaje a cifrar, como veremos en el ejemplo. Lo que se hace, es tomar la letra de la clave que se corresponda con la letra a cifrar y buscar su equivalente alfabeto de César que comienza con dicha letra. Para descifrar, lógicamente hay que conocer la clave y operar en sentido inverso.

Figura 13. B. Vigenère (1523-1596)

Tablero de Vigenère

0	**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**
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	**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**
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	**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**
21	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
22	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
23	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
24	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
25	**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**

Para cifrar se procede de la siguiente manera:

a) Se busca una palabra clave fácil de recordar.

b) Se escribe la palabra debajo del texto en claro, repitiéndose tantas veces como sea necesario.

c) Cada letra del texto en claro se codifica con el alfabeto de la tabla marcado por la letra inferior, o sea, la letra de la clave que corresponde.

Ejemplo:

clave = **AZUL**

Texto a remitir: **el ejército está preparado**

Proceso: Se escribe le clave debajo del texto a cifrar.

E	L	E	J	E	R	C	I	T	O	E	S	T	A	P	R	E	P	A	R	A	D	O
A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U

Por último, cada una de las letras del mensaje se transforma en otra.

Así la E, se cifra como la E (del alfabeto A), la L se cifra como la K(del alfabeto Z), la E, se cifra como Y, y así sucesivamente... El mensaje cifrado es: **EK YUEQWTTN YDTZ JCEOUCACI**

Las investigaciones de Blaise de Vigénere, así como los métodos utilizados en su época están recogidos en su libro *Traicté des Chiffres*, publicado en 1586. Curiosamente un sistema tan avanzado fue ignorado durante casi dos siglos. Seguramente las razones para no utilizar la cifra de Vigénere son varias: el uso extendido, por parte de los criptógrafos, de las cifras monoalfabéticas, añadiendo homófonos y sobretodo la dificultad de utilizar las cifras polialfabéticas.

3.4.2. Los Rossignol y la Gran cifra

Antoine y Bonaventure Rossignol, padre e hijo respectivamente, alcanzaron fama cuando en el año 1626 descifraron una carta, remitida por el ejercito hugonote, y capturada por los franceses. Su éxito fue de tal magnitud que el padre y el hijo, como recompensa, sirvieron a los reyes Luis XIII y Luis XIV como geniales criptoanalistas. Su concienzudo y meticuloso trabajo les llevó a comprender mejor distintas técnicas criptográficas, proponiendo ellos mismos un sistema que se ha conocido en la literatura como **La Gran Cifra**. Al morir los Rossignol la Gran Cifra cayó en deshuso. Sin embargo, era tan sólida e indescifrable que desafió los esfuerzos de varias generaciones de criptoanalistas. Por fin, a finales del siglo XIX, un comandante militar, experto del departamento Criptográfico del ejercito francés, llamado **Etienne Bazeries** (1846-1931) fue capaz de descifrar la Gran Cifra después de arduos años de trabajo.

Figura 14. E. Bazeries (1846-1931)

3.4.3. El Código Morse

El código Morse no es una forma criptográfica, en realidad no trata de ocultar el mensaje. No es otra cosa que un alfabeto alternativo que va muy bien para trasmitir mensajes de una

manera sencilla. Si queremos transmitir un mensaje secreto, mediante el código Morse, es necesario codificarlo antes de remitírselo al telegrafista de turno. La famosa cifra Vigenère se convirtió en una de las mejores formas de asegurar los secretos, por esta razón se la conoce también con el sobrenombre de "le chiffre indéchiffrable".

Símbolos del código Morse Internacional

SIGNO	CÓDIGO	SIGNO	CÓDIGO	SIGNO	CÓDIGO	SIGNO	CÓDIGO
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	- - . .		
1	. - - - -	2	. . - - -	3	. . . - -	4	. . . . -
5	. . . . .	6	-	7	- - . . .	8	- - - . .
9	- - - - .	0	- - - - -				

Signos habituales		
. Punto:	. - . - . -	(AAA)
, Coma:	- - . . - -	(GW)
¿ Interrogación:	. . - - . .	(UD)
= Guión doble:	- . . . -	(TV)
- Guión sencillo:	- . . . . -	(NV)
/ Raya de fracción:	- . . - .	(NR)
" Comillas:	. - . . - .	(RR)

3.4.4. Charles Babbage

Charles Babbage (1791- 1871) es uno de los grades genios del siglo XIX, matemático inglés y científico protoinformático. Es la primera persona que concibe la idea de lo que hoy llamamos ordenador. Dedicó buena parte de su vida a diseñar diversos artilugios mecánicos. A partir de 1820, Charles Babbage se interesó en el diseño y construcción de distintas máquinas de calcular. Con la ayuda económica de la condesa Ada Byron, hija del poeta Lord Byron, desarrolla el concepto de 2 calculadoras mecánicas o "máquinas de números".

La primera de ellas, llamada la Máquina en diferencias era un dispositivo mecánico que resolvía ecuaciones polinómicas por el método diferencial. La segunda, denominada Máquina Analítica[7], fue diseñada como un dispositivo de cómputo general. Ambos equipos eran totalmente mecánicos, usaban ejes, engranajes y poleas para poder ejecutar los cálculos. Ninguna de las dos máquinas las llegó a construir en su totalidad.

Actualmente en el Museo de Ciencias de Londres se exhiben partes de sus mecanismos inconclusos. El año 1991, siguiendo los planos originales de Babbage, se construyó su famosa Máquina Diferencial (un ingenio concebido originariamente por J. H. Mueller en 1786 pero que nunca tomó forma física). La máquina, empleando materiales y tecnología del siglo XIX, fue capaz de funcionar perfectamente.

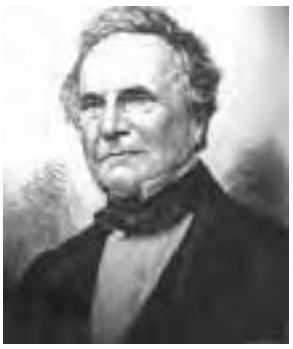


Figura 15. Charles Babbage

Figura 16. Maqueta de una porción de la máquina de diferencias

En lo que respecta a criptografía, Charles Babbage también logró resultados notables. Él fue capaz de descifrar, hacia el año 1854, la llamada cifra Vigenère. El descubrimiento de Babbage fue utilizado por los ejércitos ingleses en la guerra de Crimea, proporcionando una clara ventaja sobre los métodos criptográficos de su enemigo: el ejercito ruso. Debido a esto, sus descubrimientos sobre criptografía se ocultaron hasta su muerte y no fueron publicados hasta el siglo XX. Paralelamente a Babbage, un oficial prusiano llamado **Friedrich Kasiski** descubrió, después de varios años de trabajo, como romper la famosa cifra Vigenère. Durante décadas, Kasiski fue reconocido oficialmente como el descifrador de "le chiffre indéchiffrable".

3.4.5. La cifra del barón Lyon Playfair

El cifrado de Playfair en realidad fue inventado, el año 1854, por su amigo **Charles Wheatstone**. Se utilizaba esencialmente en comunicaciones telegráficas secretas; no obstante el procedimiento se le atribuye a su amigo el científico y barón **Lyon Playfair**.

Este sistema fue utilizado por el Reino Unido en la Primera Guerra Mundial. El sistema consiste en separar el texto en claro en diagramas y proceder a su cifrado de acuerdo a una matriz alfabética de dimensiones 5 X 5 en la cual se encuentran representadas las 26 letras del alfabeto inglés, aunque para una mayor seguridad se puede agregar una palabra clave.

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**

Matriz de Playfair original (sin clave)

Matriz de Playfair

Añadiendo una palabra clave a la matriz de cifrado se consigue una mayor seguridad. La clave se coloca al comienzo de la matriz y a continuación el resto de las letras del alfabeto.

Para cifrar es necesario seguir las siguientes reglas:

1. El mensaje a cifrar (mensaje claro) se divide en pares de letras, o dígrafos.

2. Las dos letras de todos los dígrafos deben ser diferentes, lo que se consigue insertando una "x" adicional cuando sea necesario para romper la igualdad.

Ahora se mira a la tabla de Playfair, pudiéndose dar los siguientes casos:

3. Las dos letras del dígrafo están en la misma fila y diferente columna, en ese caso, para cifrarlas, se desplaza cada letra una columna a la derecha. (si una de las letras está al final de la fila se reemplaza por la letra que hay al principio de fila).

$$(a_{ij}; a_{ik}) \longrightarrow (a_{ij}+1; a_{ik}+1)$$

4. Las dos letras del dígrafo están en la misma columna y diferente fila, en ese caso, para cifrarlas, se desplaza cada letra una columna hacia abajo.

(si una de las letras está al final de la columna se reemplaza por la letra que hay al principio de columna)

$$(a_{ik}; a_{jk}) \longrightarrow (a_{(i+1)k}; a_{(j+1)k})$$

5. Las dos letras del dígrafo están en filas y columnas diferentes Se realiza la siguiente operación [8]:

$$(a_{ki}; b_{js}) \longrightarrow (a_{ks}; b_{ji})$$

Ejemplo:

Clave: **mar**

Mensaje en claro : **se ha mareado hoy**

Proceso a seguir: se-ha-ma-re-ad-oh-oy (división en dígrafos)

Matriz de Playfair:

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

se (las dos letras están en filas y columnas distintas) se transforman en **QF**

ha (las dos letras están en filas y columnas distintas) se transforman en **EC**

ma (las dos letras están en la misma fila y diferente columna) se transforman en **AR**

re (las dos letras están en filas y columnas distintas) se transforman en **AF**

ad (las dos letras están en filas y columnas distintas) se transforman en **ME**

oh (las dos letras están en la misma columna y filas distintas) se transforman en **UO**

oy (las dos letras están en filas y columnas distintas) se transforman en **NZ**

Por tanto el mensaje cifrado es: QF-EC-AR-AF-ME-UO-NZ

3.4.6. La Cifra ADFGVX

A finales del siglo XIX el italiano G. Marconi inventó una forma de comunicarse prodigiosa: la radio. En manos de los militares la radio fue un poderoso medio de transmisión, pero los mensajes podían caer también en manos enemigas, por lo que era necesario mandarlos cifrados.

La Primera Guerra Mundial fue una guerra a gran escala, por lo que era necesario disponer de una codificación rápida y efectiva. Una de las cifras más famosas fue la llamada **Cifra ADFGVX**, introducida por los alemanes en el invierno de 1918. La cifra es una mezcla de métodos de sustitución y de trasposición, esto hace que su desciframiento sea verdaderamente complicado.

Cifrar mediante ADFGVX

Se empieza disponiendo las 26 letras del alfabeto anglosajón y los diez dígitos en una matriz 6x6. Las líneas y las columnas van encabezados por las letras **A D F G V X**. El modo de ordenar letras y número, en la cuadrícula forma parte de la clave y necesita ser comunicada al receptor del mensaje. Su ordenación es aleatoria.

Ejemplo:

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

En primer lugar tomaremos cada letra del mensaje en claro sustituyéndola por las letras correspondientes a su fila y columna. Por ejemplo el número 4 sería sustituido por las letras FA y la k por el par de letras VX.

Veamos como se cifra el siguiente mensaje: **envien municiones**

Acudiendo a la matriz anterior , tenemos:

Mensaje cifrado: **VVFGGFXFVVFGDADDFGXFAXXFXGFGVVXD**

Hasta aquí es solo un cifrado ordinario por sustitución, que se descifra con un análisis de frecuencia si se dispone de suficiente texto. Sigue otra fase con una trasposición dependiente de una palabra clave. Supongamos que la clave es **WHISKY**. Las letras de la **clave** se escriben en la cabecera de una cuadrícula. El texto que hemos cifrado antes se escribe por filas en dicha cuadrícula así:

W	H	I	S	K	Y
V	V	F	G	G	F
X	F	V	V	F	G
D	A	D	D	F	G
X	F	A	X	X	F
X	G	F	G	V	V
X	D	A	A	A	A

Donde hemos añadido dos caracteres de relleno (AA) para que el cuadro quede completo. Ahora las columnas de la cuadrícula se cambian de posición de modo que las letras de la clave queden en orden alfabético:

H	I	K	S	W	Y
V	F	G	G	V	F
F	V	F	V	X	G
A	D	F	D	D	G
F	A	X	X	X	F
G	F	V	G	X	V
D	A	A	A	X	A

Para acabar leemos por columnas la cuadrícula y el resultado es el texto cifrado:
VFAFGDFVDAFAGFFXVAGVDXGAVXDXXXFGGFVA

Si trasmitimos este texto cifrado mediante un código Morse o similar, la posibilidad de desciframiento es muy baja, puesto que el mensaje consta de únicamente 6 letras.

Ese mismo año, exactamente el 2 de Junio de 1918, el criptoanalista francés **Georges Painvin**, fue capaz de descifrar un mensaje mediante la cifra ADFGVX

Figura 17. G. Painvin (1886-1980)

3.4.7. Auguste Kerckhoffs y sus reglas

La Primera Guerra Mundial marcó toda una época en la criptografía. Los criptoanalistas franceses eran, sin duda, los más perspicaces. El holandés **Auguste Kerckhoffs**, aunque educado en Francia, estudió a fondo los distintos sistemas criptográficos, publicando sus investigaciones en un artículo titulado *la cartografía militar*.

Kerckhoffs recomienda, en su artículo, que los sistemas criptográficos cumpliesen las siguientes reglas, que efectivamente han sido adoptadas por gran parte de la comunidad criptográfica, son las siguientes:

Reglas de Kerckhoffs

Referidas a reglas militares aceptadas mundialmente:

1. No debe existir ninguna forma de recuperar el texto claro a partir del criptograma (seguridad ante el primer ataque).
2. Todo sistema criptográfico debe estar compuesto por dos tipos de información:
   a. **Pública:** se refiere a la familia de algoritmos que definen el sistema criptográfico.
   b. **Privada:** es conocida sólo por el usuario. La clave de cifrado de cada usuario en particular.
3. La forma de escoger la clave debe ser fácil de recordar y modificar.
4. Debe ser posible la comunicación del criptograma con los medios de transmisión habituales.
5. La complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido (el costo es proporcional al secreto que quiere guardar).

Tipos de Secreto

En criptografía se definen varios niveles de seguridad en los cuales se pueden enmarcar los diferentes algoritmos criptográficos:

1. **Secreto Perfecto:** El mensaje es seguro frente a tiempo y recursos ilimitados.
   En este tipo de cifrado el tamaño de la clave es mayor o igual que el tamaño del texto a cifrar.
2. **Secreto Computacional:** El mensaje es seguro frente a ataques con tiempo y recursos limitados.
   Ejemplo: Criptosistemas de clave pública.
3. **Secreto Probable:** El mensaje se encuentra probablemente seguro.
   Ejemplo: Criptosistemas de clave privada.
4. **Secreto condicional:** La seguridad del mensaje depende de las características de sus entorno.
   Ejemplo: Un mensaje no cifrado o cifrado utilizando criptosistemas clásicos, que se envía a través de una red "segura".

3.5. Máquinas y artilugios criptográficos

Las primeras máquinas de criptografiar son los famosos discos de León Alberti. Él construyó dos discos concéntricos, de cobre, sobre los que estaban rotulados el alfabeto. Los dos discos giran de manera independiente y se utilizan para codificar los mensajes. En esencia, lo que realmente hacen es un ciframiento de César.

Figura 18. Tres tipos de Discos de Alberti

El americano **Thomas Jefferson** (1743-1826), autor de la Declaración de Independencia de E.U.A. ideó una máquina para criptografiar mensajes, aunque el primero en fabricarla en serie fue Etienne Bazeries, en 1891. El aparato consiste en una serie de discos que giran alrededor de un mismo eje y llevan impresas las letras del alfabeto, dispuestas en distintos órdenes. El emisor mueve los discos hasta poner en línea las letras que necesita para escribir el mensaje. Entonces lo codifica transmitiendo las letras que hay en cualquier otra línea. Para descodificar el mensaje, el receptor coge su propia rueda y pone las letras del código en orden. Después no tiene más que buscar la línea de letras con el mensaje enviado. La máquina se conoce con el nombre de **cilindro de Jefferson**.

Figura 19. Cilindro de Jefferson

En un cilindro de Jefferson más sencillo podemos ver su funcionamiento:

En el dibujo anterior vemos el resultado de cifrar el texto llano: **secretword**, su resultado es decir **mvdtswxhx**.

Sin duda, el mayor desarrollo de artilugios criptográficos se dio en el periodo de entreguerras por la necesidad de establecer comunicaciones militares y diplomáticas seguras. En 1940, se construyó la máquina **Hagelin C-48** consistente en seis volantes unidos por el eje y con distinto número de dientes.

Fig 12. Hagelin C-48.

En la Segunda Guerra Mundial se construyó por parte alemana la famosa máquina **Enigma**, que se basaba en un perfeccionamiento del cilindro de **Jefferson**. La máquina británica **Colossus** diseñada por matemáticos ingleses, dirigidos por Alan Turing, logró desenmascarar las claves de Enigma.

Fig13. Enigma.

El 1 de junio de 1944 la máquina **Colossus** interceptó un mensaje crucial: Hitler y su Alto Mando esperaban un ataque aliado masivo en Calais. Esto determinó que el general Eisenhower decidiera desembarcar sus tropas el 6 de junio en las playas de Normandia. El efecto sorpresa multiplicó el golpe sobre la defensa germana. Este hecho, junto al éxito descifrador de la máquina **Colossus**, supuso, según un artículo de *The Guardian*, de 1995, un acortamiento de la guerra de por lo menos dos años[9].

Los americanos construyeron también la máquina **Magic** utilizada para descifrar el código púrpura japonés ; igualmente usaron a los indios navajos, con su difícil lenguaje, para la transmisión de mensajes.

Para acabar

Con el desarrollo de la informática en la segunda mitad del siglo pasado y con el uso cada vez más extendido de las redes informáticas y del almacenamiento masivo de información se ha dado paso a un gran salto en el estudio de sistemas criptográficos.

En 1975 Diffie y Hellman establecieron las bases teóricas de los algoritmos de clave pública, hasta entonces no se concebía un sistema de cifrado que no fuese de clave secreta. En la actualidad se usan distintos métodos criptográficos, el **DES** (de clave secreta), método **RSA**, método de Merkle y Hellman, etc... Pero eso será motivo de otro artículo que se publicará el próximo número de SIGMA.

BIBLIOGRAFÍA

Caballero, P. (2002): *Introducción a la Criptografía*. Ed. Ra-Ma. Madrid.

Feregrino, C. (Julio 2003): *Apuntes sobre Compresión Criptografía de Datos*.

Galende, J.C. (1995): *Criptografía: Historia de la escritura cifrada*. Ed. Complutense,. Madrid.

Gardner, M. (1990): *Mosaicos de Penrose y Escotillas Cifradas*. Ed. Labor.

Kahn, D. (1996): *The Codebreakers*. Scribner. New York.

Newton, D.E. (1997): *Encyclopedia of Cryptology*. ABC-Clio. Santa Bárbara.

Sgarro, A. (1989): *Códigos secretos*. Pirámide.

Singh, S. (2000): *Los códigos secretos*. Ed. Debate.

NOTAS

(1) 1. Criptología pre-científica, abarca hasta mediados del siglo XX; más que una ciencia se considera un arte.

2. Criptología científica: inicia en 1949, cuando Shannon logró cimentar la criptografía sobre bases matemáticas. Entonces surgieron los denominados criptosistemas de clave secreta, los cuales pueden ser calculados a partir del descifrado, y viceversa. En la mayoría de estos sistemas, las claves coinciden, y por supuesto han de mantenerse como un secreto entre emisor y receptor.

3. Criptología de clave pública, surge a partir de 1977.

(2) Como norma general se suelen poner en minúsculas las letras del alfabeto original, y en mayúsculas las correspondientes al alfabeto cifrado.

(3) En el libro de Simon Singh (pág. 36-41) se puede ver un ejemplo resuelto siguiendo las normas de Al Kandi.

(4) La idea de una sustitución polialfabética es la siguiente: Para cifrar un mensaje, se usa una mezcla de diferentes sustituciones monoalfabéticas, que se pueden codificar por medio de una clave. El resultado final es que la misma letra del texto original puede acabar representada por diferentes letras en el texto cifrado. Esto bloquea los intentos del criptoanalista desde el punto de vista estadístico.

(5) Técnicamente, un código se define como una sustitución al nivel de as palabras o frases codificadas.

(6) Un nomenclator es un sistema de codificación que se basa en el alfabeto cifrado, el cual se utiliza para codificar la mayor parte del mensaje, y en una lista limitada de palabras o frases codificadas.

(7) La Máquina Analítica es considerada como el primer calculador numérico universal, en el que se recogían los elementos de la moderna computadora, de ahí que se le reconozca a Babbage como el auténtico padre de los ordenadores.

(8) Para codificar la primera letra se mira en su fila hasta llegar a la columna que contiene la segunda letra, la letra en esa intersección cifrará a la primera letra. La segunda letra es reemplazada por la correspondiente letra que ocupa el lugar de la columna de la primera letra y de la fila de la segunda.

(9) Enigma fue el secreto mejor guardado de la II Guerra Mundial después de la bomba atómica. Basándose en una patente holandesa, el servicio de información alemán creó la máquina de codificación de mensajes más avanzada hasta la llegada del ordenador. En los años 30, matemáticos polacos trabajaron para anular el poder de Enigma, pero ésta se imponía con nuevos avances. Los polacos entregaron el testigo y sus conocimientos al servicio del espionaje británico, que en Bletchley Park, al norte de Londres, reunió a las mejores mentes aliadas para destapar el misterio. Y lo lograron: el día anterior al Desembarco de Normandía comenzó a funcionar Bomba, una máquina que descifraba los mensajes de la Marina germana, que poseía la Enigma más avanzada.
Un artículo publicado en *The Guardian* en 1995 aseguraba que sin el trabajo de Bletchley Park la guerra habría durado dos años más. Además de salvar vidas, el trabajo anti-Enigma llevó a la creación de Colossus, para los británicos la primera computadora del mundo.

Autor: Vicente Meavilla