HISTORIA DE LA ESCRITURA

LA ESCRITURA CIFRADA

Antonio Sánchez González
Profesor Titular de Ciencias y Técnicas Historiográficas de la Universidad de Huelva, GI Hum-340 Patrimonio Documental y Bibliografico de Andalucia y America: Fuentes Para Su Estudio; antonio.sanchez@dhis2.uhu.es

"Un efecto esencial de la elegancia es ocultar sus medios"
Honoré de Balzac

La *Criptografía* (del griego criptos = oculto + graφh = escritura), significa literalmente «escritura oculta» y alude a la escritura secreta o cifrada. Se trata, pues, de la técnica o arte de cifrar y descifrar información utilizando técnicas que hacen posible el intercambio de mensajes de manera que solo puedan ser leídos por las personas a quienes van dirigidos.

El principio básico de la Criptografía es, por tanto, mantener la privacidad de la comunicación entre dos personas alterando el mensaje original de modo que sea incomprensible a toda persona distinta del destinatario; a esto debemos la autenticación, esto es, la firma del mensaje de modo que un tercero no pueda hacerse pasar por el emisor.

A la transformación del mensaje original en el mensaje cifrado (criptograma) le llamamos "cifrado", y a la operación inversa, le llamamos "descifrado"; estos pasos se realizan mediante un conjunto de reglas preestablecidas entre los comunicantes que llamamos "clave". El "criptoanálisis" es el conjunto de técnicas que intenta encontrar la clave utilizada entre dos comunicantes, desvelando así el secreto de su correspondencia.

DIFERENTES FORMAS DE ESCRITURA CIFRADA EN LA ANTIGÜEDAD Y LA EDADMEDIA

Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes, especialmente durante las campañas militares, de forma que, si el mensajero era interceptado, la información que portaba no corriera el peligro de caer en manos del enemigo. Desde la **Antigüedad**, pues, se utilizaron varios procedimientos para velar u ocultar la escritura: caso, por ejemplo, de tatuar un mensaje en la cabeza afeitada al mensajero —generalmente un esclavo— para después dejarle crecer el pelo y enviar así el mensaje oculto; caso también de escribir mensajes en tablas que luego eran cubiertas con cera, de forma que parecían no haber sido usadas. Pero fundamentalmente se dieron estos tres tipos o sistemas de escrituras criptográficas:

a) Invisible. Es la que escapa a la vista de cualquier persona, utilizando fórmulas como la descomposición de *tintas simpáticas* que impedían ver la escritura. Estos mensajes secretos se escriben, por lo general, entre las líneas de una carta realizada con tinta común, para que no llamara la atención una hoja en blanco. También solían escribirse la información importante en el dorso o los márgenes de la propia carta. Era habitual el uso de vinagre, zumos de frutas u orina. Al calentar el papel, la escritura oculta se hace visible.
b) Disimulada. Es la que presenta un texto a la vista con un significado aparente y distinto al de la comunicación.

c) Cifrada. Es la que su texto carece de significado aparente, ocultándose el significado real de los signos escritos. Puede afectar a letras, grupos de letras, sílabas, palabras, frases, etc. o hacerse de manera híbrida.

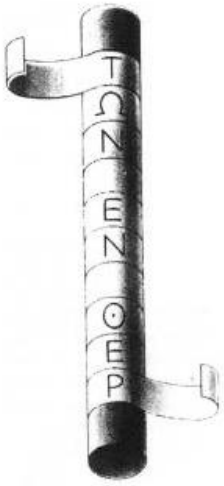
Para ocultar el significado real se recurrió a dos procedimientos en la Antigüedad:

Uno era el llamado *método de trasposición*, que consiste en ocultar la relación de significado entre varias palabras de modo que, para la intelección del texto, se hacía preciso el cambio de posición o la inversión de los elementos del texto a la vista.

Algunos pueblos antiguos utilizaron trozos de cuero con escritos en aparente desorden con espacios interlineales constantes; al enrollar esas tiras en espiral en una barra cilíndrica de longitud y diámetro convenidos que servía como clave, las letras se yuxtaponían desvelando el verdadero significado del texto.

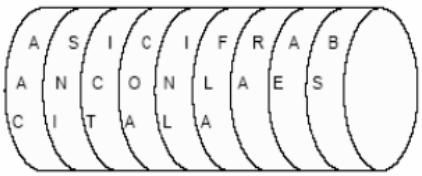
La escitala espartana **(siglo V a.C.)**

Fue el procedimiento usual empleado por los griegos lacedemonios en el siglo V a. C. durante las guerras del Peloponeso con la "*escitala espartana*". Es decir, el cifrado se basaba en la alteración del mensaje original mediante la inclusión de símbolos innecesarios que desaparecían al enrollar el mensaje en un rodillo (la *escitala*), de longitud y grosor prefijados. Aun sabiendo la técnica utilizada, si no se tenían las dimensiones exactas de ese rodillo, un posible interceptor del mensaje tenía muy difícil su criptoanálisis. El grosor y la longitud de la escitala eran la clave de este sistema. Al desenrollar la cinta, el mensaje quedaba cifrado.



Cilindro o escitala espartana

El otro procedimiento es el *método de sustitución*, que consiste en dejar en su orden primitivo las letras y palabras del texto pero sustituyéndolas aisladamente por un signo que figura en una tabla de concordancias previamente fijadas.



Mensaje: "*Así cifraban con la escitala*". Cualquiera que desenrollara la tira se encontraría con:
- AAC SIN ICT COA INL FLA RA AE BS.

La sustitución puede hacerse de modo que un signo funcione con un significado único o que adquiera la significa-ción de varias letras o palabras.

El cifrado de Polibio **(siglo II a.C.)**

Es el cifrador por sustitución más antiguo que se conoce; se llama así porque fue documentado por el historiador griego Polibio.

El método se basaba en la posición de las letras en una tabla secreta, en cuyos ejes se ponían diferentes combinaciones de letras o números y dentro de la tabla las letras del alfabeto. Cada letra del mensaje a cifrar era sustituida por sus "coordenadas".

Se ve bastante más claro en el siguiente ejemplo:

	A	B	C	D	E
A	a	b	c	d	e
B	f	g	h	i/j	k
C	l	m	n	o	p
D	q	r	s	t	u
E	v	w	x	y	z

Mensaje: "Polybios es el rey"
Criptograma:
CECDCAEDABBDCDDC AEDC AECA DBAEED

Cifrado de César **(siglo I a.C.)**

También los romanos utilizaron sistemas de sustitución, siendo uno de los más conocidos el llamado *cifrado de César* porque

supuestamente lo utilizó Julio César en sus campañas militares. Eso es, al menos, lo que afirma Suetonio[47]:

"Si tenía que decir algo confidencial, lo escribía usando el cifrado, esto es, cambiando el orden de las letras del alfabeto, para que ni una palabra pudiera entenderse. Si alguien quiere decodificarlo, y entender su significado, debe sustituir la cuarta letra del alfabeto, es decir, la D por la A, y así con las demás" (Suetonio, *Vida de Julio César*, 56).

Este sistema criptográfico tiene, por tanto, como algoritmo el desplazamiento de tres espacios hacia la derecha de los caracteres del texto en claro.

Así, si se trataba del empleo de letras del alfabeto latino clásico, se sustituía el texto en claro por las que correspondían a esos tres lugares abajo en el orden alfabético (Ej. "FZP" por "cum").

Texto claro: A B C D E F G H I K L M N O P Q R S T V X Y Z

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

Se trata, pues, de un criptosistema de sustitución monoalfabético por desplazamiento, en el que las operaciones se realizan módulo *n*, siendo *n* igual al número de elementos del alfabeto. Veamos otro ejemplo del alfabeto castellano:

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

Alfabeto de cifrado del César para castellano módulo 27

Mensaje: Tú también, Brutus?

Criptograma: wx wdoelhp euxwxv?

En la **Edad Media**, aunque pusiera de manifiesto Bischoff que se produjo una notable afección por la escritura cifrada, ciertamente después del siglo I antes de Cristo y hasta el siglo XV de nuestra era, no se conoce ningún sistema criptográfico de nueva invención digno de resaltar. Por eso a esta etapa se la conoce como "edad oscura" de la Criptografía.

San Bonifacio (672-754) es tenido por el introductor de un doble sistema de sustitución (muy rudimentario, por cierto, y de fácil identificación):

-uno reemplazando las vocales por puntos, de este modo:

[a=: e=: i=. o=:: u=:.:]

-y el otro sustituyéndolas por las consonantes que le siguen en el orden alfabético

[b=a f=e k=i p=o x=u]

Con mayor o menor complejidad sistemas similares fueron habituales hasta el siglo XIV, en que éstos comienzan a perfeccionarse.

Ya en el siglo XV se va a utilizar por primera vez un método criptográfico de tipo polialfabéti-co, conocido como "disco de Alberti".

***Disco de Alberti* (1466)**

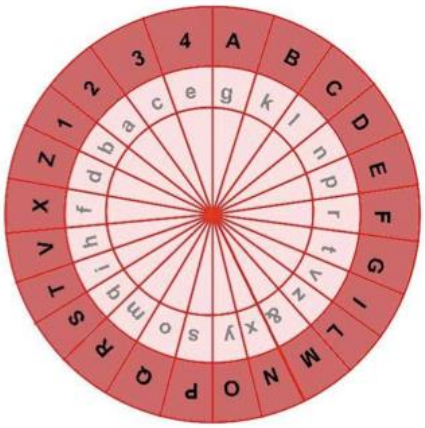
León Battista Alberti (1404-1472) –el célebre músico, pintor, escritor y arquitecto italiano del Renaci-miento–, concibió en 1466 el primer sistema polialfabético que se conoce, que emplea varios

[47] Aunque hay autores que afirman que, en realidad, Julio César nunca utilizó este sistema de sustitución y que, aún así, su atribución ha tenido tanto arraigo que el nombre de este método ha pervivido hasta nuestros días, sin embargo, existen indicios de que César usó también sistemas criptográficos más complicados pues el escritor Aulus Gellius hace referencia a un tratado (perdido) sobre el cifrado de sus cartas: "…*Hay incluso un tratado ingeniosamente escrito del gramático Probus referente al significado secreto de las letras en la composición de las epístolas de César*".

abecedarios, utilizando uno u otro, cada tres o cuatro palabras[48]. El emisor y el destinatario habían de ponerse de acuerdo para fijar la posición relativa de dos círculos concéntricos, que determinara la correspondencia de los signos. Los diferentes abecedarios utilizados eran representados en uno de los discos, mientras que el otro se rellenaba con el abecedario normal, más los números del 1 al 4. Este disco define 24 posibles sustituciones dependiendo de la posición del disco interior.

Una vez establecida la correspondencia entre caracteres de ambos discos, se sustituye el texto en claro del disco exterior por cada una de las letras correspondientes del disco interior, cambiando al abecedario correspondiente (prefijado por los comunicantes) cada *x* palabras, habiendo sido *x* también prefijada por los comunicantes.

[48] Algunas de las máquinas, posteriores al disco de Alberti, y por lo tanto algo más complicadas, que también utilizarán un sistema propio de encriptación polialfabético son: la *Enigma* (inventada por Arthur Scherbius en 1923 y usada por los alemanes durante la II Guerra Mundial); las de *Hagelin* (desarrolladas por el criptólogo sueco Boris Hagelin entre 1920 y 1930, que se basaban en el llamado sistema de cifrado de Beaufort; y la *máquina M-325* (inventada por Frederick FriedMan en los años cuarenta del siglo XX, que es muy parecida a la Enigma alemana, ya que también se basa en rotores que realizan una sustitución polialfabética).



Disco de Alberti

DIFERENTES FORMAS DE ENCRIPTADO DE LA INFORMACIÓN CONFIDENCIAL DURANTE LA EDAD MODERNA

A fines del Medievo y comienzos de la Edad Moderna la Criptografía alcanza un auge importante como consecuencia de la aparición de los Estados Modernos (donde la diplomacia adquirió un papel muy destacado en las relaciones internacionales), convirtiéndose en verdadera obra de arte.

Entre los procedimientos y sistemas de cifrados que entonces se idearon sobresalen éstos:

-el uso de números arábigos que, en pareja, reemplazaban a las vocales y a las consonantes fáciles de descifrar, e incluso para complicar más la identificación, cada vocal y cada consonante podía tener varios signos y combinaciones.

-el ideado por el monje alemán *Johann Heidenberg (Trithemius)* a principios del siglo XVI, consistente en un tablero de alfabetos superpuesto que manejaba a través de una clave establecida. Es autor de varias obras de codificación de mensajes, destacando su célebre *Steganographia* o ciencia para ocultar las escrituras[49].


STEGANOGRAPHIA:
ARS PER OCCUL
JOANNE TRITHEMIO,
INCIPIT LIBER PRIMUS
STEGANOGRAPHIÆ
JOANNIS TRITHEMII,
SERENISSIMUM PRINCIPVM, DOMINVM
PHILIPPVM, COMITEM PALATINUM

Johannes Trithemius. *Steganographia* ('Escritura Oculta')

[49] Johannes Trithemius, conocido como Johann von Heidenberg (1462-1516) fue el fundador de la sociedad secreta *Sodalitas Celtica* (Cofradía Céltica) —dedicada al estudio de las lenguas, las matemáticas, la astrología y la magia de los números—. Es autor de la famosa *Steganographia* o ciencia para ocultar mensajes, obra publicada originalmente en 1500 (la edición del año 1606, única conocida, aparece ya incompleta), y de una *Polygraphia* (1518), compleja obra dedicada a la codificación de mensajes. Su primer libro contiene nada menos que 376 alfabetos de 24 letras, el segundo libro presenta otros 1.176 alfabetos en tres columnas, lo que forman 3.528 dicciones de una lengua universal mientras que el tercer libro muestra 132 alfabetos de dicciones inventadas, a las que hay que quitar la segunda letra de cada palabra para escribir mensajes en clave... Según ciertos autores, ambas no son sino una única obra presentada en dos partes diferenciadas: la primera es metafísica y teórica, la segunda es práctica.

Blaise de Vigenère

Otro de los criptógrafos más importantes del siglo XVI fue el francés *Blaise de Vigenère* (1523-1596), diplomático francés, cuyo interés inicial en la criptografía era meramente práctico y se relacionaba con su trabajo. Después, a la edad de treinta y nueve años, Vigenère decidió que ya había acumulado suficiente dinero como para abandonar su carrera diplomática y dedicar su vida al estudio. Fue sólo entonces cuando estudió en detalle las ideas de Alberti, Trithemius y otros, combinándolas hasta lograr una nueva cifra, coherente y poderosa, que divulgó en su *Traité des chiffres où secrètes manières d'escrire* (1586). Esta nueva cifra ha llegado a nuestros días asociada a su nombre. La fuerza de la *cifra Vigenère* radica en que no utiliza uno, sino 26 alfabetos cifrados distintos para cifrar un mensaje.

***Cifrado de Vigenère* (1586)**

Se trata de un sistema criptográfico polialfabético o de sustitución múltiple, de clave privada o secreta. Este tipo de criptosistemas aparecieron para sustituir a los monoalfabéticos o de sustitución simple, basados en el algoritmo de Cesar que hemos visto anteriormente, que presentaban ciertas debilidades frente al ataque de los criptoanalistas relativas a la frecuencia de aparición de elementos del alfabeto.

El principal elemento de este sistema es la llamada "tabla de Vigenère", una matriz de caracteres cuadrada, que se muestra a continuación:

	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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

Tabla de Vigenère

Para el proceso del cifrado, el mensaje a cifrar en texto claro ha de descomponerse en bloques de elementos (letras), del mismo tamaño de la clave y aplicar sucesivamente la clave empleada a cada uno de estos bloques, utilizando la tabla anteriormente proporcionada, perteneciendo las letras de la clave a la columna de la izquierda.

Un ejemplo podría ser el siguiente, utilizando como clave la palabra "*prueba"* y como mensaje en claro "*cifrado de Vigenère*":
Este método de cifrado poli-

C	I	F	R	A	D	O	D	E	V	I	G	E	N	E	R	E
P	R	U	E	B	A	P	R	U	E	B	A	P	R	U	E	B

Cifrado: R Z Z V B D D U Y Z J G T E Y V F

alfabético se consideraba invulnerable hasta que en el siglo XIX se consiguieron descifrar algunos mensajes codificados con este sistema, mediante el estudio de la repetición de bloques de letras: la distancia entre un bloque y su repetición suele ser múltiplo de la palabra tomada como clave.

Ya en el siglo XVII, a *Gustavus Selenus*, pseudónimo del duque alemán Augusto II de Brunswick-Lüneburg, se le debe la obra "Cryptomenytices et Cryptographiae" (1624)[50]. En ella, Selenus presenta una complejidad, desconocida hasta entonces, empleando una rueda que permite hacer girar una veintena de círculos concéntricos, cada uno de los cuales contienen dupletes (grupos de dos palabras), así como tablas que contienen unos treinta mil tripletes.

En la corte francesa de Luis XIV y Richelieu, se utilizó otro procedimiento criptográfico compuesto por *Antoine Rossignol* y su hijo *Bonaventure*, conocido por la *Gran Cifra de Luís XIV*, a base de grupos de números para designar letras, sílabas, palabras frecuentes, números y nombres propios; era prácticamente indescifrable, hasta el punto que no se consiguió interpretar hasta fines del siglo XIX[51].

Igualmente se idearon en el siglo XVII los denominados sistemas de «repertorios» o «nomenclatores» —también llamados «códigos» o «tablas cifradoras»—, libros con un número más o menos elevado de palabras o frases adecuadas al uso destinado, a cada una de las cuales corresponde una cifra compuesta, por lo general, de una a cuatro o cinco letras del alfabeto y/o números arábigos. Por consiguiente, la diferencia esencial entre el «nomenclátor» y el «diccionario» estriba en que éste procura abarcar todas las palabras, en tanto que aquél recoge sólo un número limitado de ellas.

[50] Augusto II de Brunswick-Lüneburg o *Gustavus Selenus* (en español sería algo así como "El hombre en la Luna"), era un aficionado a la criptografía y el ocultismo, que publicó en su obra criptográfica "Cryptomenytices et Cryptographiae" (Lüneburg, 1624) el "Libro III" de la *Steganografía* del abad Johannes Trithemius, analizándolo aunque sin ofrecer una solución a las claves secretas que contiene (Heidel, en 1676, pretendió haber descifrado el código publicando una serie de indescifrables criptogramas cuya clave no proporcionó, por lo que jamás se ha llegado a saber si era cierto o no). El título completo de esta obra suya más conocida es *Cryptomenytices: "Gustavi Seleni Cryptomenytices et Cryptographiæ, Libri IX. In quibus & planissima Steganographiæ à Johanne Trithemio, Abbate Spanheymensi & Herbipolensi, admirandi ingenii Viro, magicè & ænigmaticè olim conscriptæ, Enodatio traditur. Inspersis ubiquè Authoris ac Aliorum, non contemnendis inventis*, nombre tan largo en el que el autor no presenta al lector duda alguna de quién fue su autor, en qué obras se basó o qué es lo que trata... En ella, como decimos, Selenus presenta la novedad de emplear una rueda que permite hacer girar una veintena de círculos concéntricos, cada uno de los cuales contienen dupletes (grupos de dos palabras), así como tablas que contienen unos treinta mil tripletes.

[51] La alteración de la cifra monoalfabética básica de diversas maneras, tales como añadir homófonos, hizo posible cifrar mensajes de forma segura, sin tener que recurrir a las complejidades de la cifra polialfabética. Uno de los ejemplos más notables de una cifra monoalfabética mejorada lo constituyó la llamada *Gran Cifra de Luís XIV*, la cual fue utilizada para cifrar los mensajes más secretos del rey, protegiendo los detalles de sus planes, conspiraciones y maquinaciones políticas. La Gran Cifra fue inventada por el equipo formado por un padre y su hijo, Antoine y Bonaventure Rossignol. Antoine había alcanzado prominencia por vez primera en 1626, cuando le entregaron una carta codificada capturada a un mensajero que abandonaba la sitiada ciudad de Réalmont. Antes de que acabara el día ya había descifrado la carta, revelando que el ejército hugonote que había mantenido la ciudad estaba a punto de caer. Los franceses, que hasta entonces no habían sido conscientes de la desesperada situación de los hugonotes, devolvieron la carta acompañada de su desciframiento. Los hugonotes, al saber ahora que su enemigo no cedería, no tardaron en rendirse. El desciframiento había tenido como resultado una cómoda victoria francesa. Las páginas cifradas contenían miles de números, pero sólo 587 diferentes.

Durante el Antiguo Régimen, como vimos ya en el caso de la corte de Luís XIV, el interés de los monarcas por la Criptografía fue notable. Después nos referiremos al cifrario de los ejércitos de Felipe II, descifrado por el matemático francés Viète para el rey galo Enrique IV[52]. Otro caso paradigmático fue el de María Estuardo, reina de los escoceses, ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquélla tras un criptoanálisis exitoso por parte de los matemáticos de Isabel.

LA CRIPTOGRAFÍA CONTEMPORÁNEA

Desde el siglo XIX y hasta la Segunda Guerra Mundial las figuras más importantes en este terreno fueron la del holandés *Auguste Kerckhoffs* [53] y la del prusiano *Friedrich Kasiski*[54].

Máquinas *Enigma* utilizadas por los alemanes durante la II Guerra Mundial

polialfabéticos, especialmente el cifrado de Vigenère (se cree que Charles Babbage obtuvo un método similar pero lo mantuvo en secreto). El método se basaba en el análisis de fragmentos repetidos de texto dentro del texto cifrado; dicho análisis permitía conocer la longitud de clave usada en el cifrado, técnica conocida como el "método Kasiski". Él se percató de la existencia de palabras repetidas en el texto cifrado, lo cual significa casi con toda probabilidad que dichas palabras no solo eran la misma antes del cifrado sino que además la clave coincidió en la misma posición en ambas ocurrencias. Sabiendo entonces que la distancia entre palabras repetidas es múltiplo de la longitud de la clave, era cuestión de buscar diferentes palabras que se repitieran y hallar su máximo común divisor, para de esta manera encontrar un múltiplo cercano a la longitud de la clave. La longitud de la clave será este número o algún factor primo del mismo. Una vez descubierta la longitud de la clave con la que se cifró el documento tan solo hay que dividir el texto en bloques del mismo tamaño que la longitud de la clave y aplicar el método estadístico tradicional del "cifrado de César".

Pero es en el siglo XX cuando la historia de la Criptografía vuelve a presentar importantes avances. En especial durante las dos contiendas bélicas que marcaron al siglo: la Gran Guerra y la Segunda Guerra Mundial. A partir del siglo XX, la Criptografía usa una nueva herramienta que permitirá conseguir mejores y más seguras cifras: las *máquinas de cálculo*. La más conocida de las máquinas de cifrado, posiblemente sea la máquina alemana *Enigma*: una máquina de rotores que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. No en vano, los mayores avances tanto en el campo de la criptografía como en el del

[52] Este importante matemático francés se hizo famoso precisamente por su hazaña de descifrar los mensajes secretos que el rey de España enviaba a su ejército en Flandes.

[53] Para el criptógrafo holandés Auguste Kerhoffs von Nieuwenhof (1835-1903), autor de uno de los libros históricos de la criptografía, *La Cryptographie militaire* (1883), la seguridad de cifrado debe residir exclusivamente en el secreto de la clave y no en el desconocimiento del algoritmo de cifrado.

[54] Friedrich Wilhelm Kasiski (1805–1881) fue oficial de infantería de las fuerzas armadas prusianas, criptógrafo y arqueólogo. En 1863 publicó su *Die Geheimschriften und die Dechiffrierkunst* ("La escritura secreta y el arte del descifrado") que fue la primera publicación sobre criptoanálisis aplicado a los cifrados de sustitución

criptoanálisis no empezaron hasta entonces.

Tras la conclusión de la Segunda Guerra Mundial, la Criptografía tiene un desarrollo teórico importante, siendo *Claude Shannon* y sus investigaciones sobre teoría de la información esenciales hitos en dicho desarrollo. Además, los avances en computación automática suponen tanto una amenaza para los sistemas existentes como una oportunidad para el desarrollo de nuevos sistemas. A mediados de los años 70 del siglo pasado el Departamento de Normas y Estándares norteamericano publica el primer diseño lógico de un cifrador que estaría llamado a ser el principal sistema criptográfico de finales de siglo: el *Estándar de Cifrado de Datos* o DES. En esas mismas fechas ya se empezaba a gestar lo que sería la, hasta ahora, última revolución de la Criptografía teórica y práctica: los *sistemas asimétricos*. Estos sistemas supusieron un salto cualitativo importante ya que permitieron introducir la Criptografía en otros campos que hoy día son esenciales, como el de la *firma digital*.

ESCRITURAS CIFRADAS EN ESPAÑA

Por las fuentes conservadas, no parece que tuvo mucha incidencia la escritura cifrada en España hasta el siglo XV.

Con anterioridad, en la *escritura visigótica*, según Jesús Muñoz y Rivero, se utilizaron tres procedimientos criptográficos:

-un alfabeto convencional de tres letras distintas a la de la escritura ordinaria (en casos emparentadas con la cursiva y en casos tomadas de la escritura taquigráfica)

-puntos en sustitución de las vocales:

[a= . e=: i=: o=:: u=:.:]

-y numerales romanos en sustitución de las vocales:

[a=X e=XX i=XXX o=X^{V} u= L]

A partir del reinado de los Reyes Católicos, con la constitución del Estado Moderno y el protagonismo de España en el concierto político del Antiguo Régimen, se inicia una nueva época para la escritura cifrada fundamentalmente en la correspondencia de valija diplomática.

Los sistemas criptográficos modernos entre los siglos XV y XVIII usaron y combinaron signos convencionales, letras, números y elementos nulos:

-Los signos convencionales son de gran variedad y, por tanto, de difícil interpretación.

-Las letras se combinan de distintos modos, formando alfabetos convencionales, o se utilizan aisladas, duplicadas, agrupadas o formando sílabas.

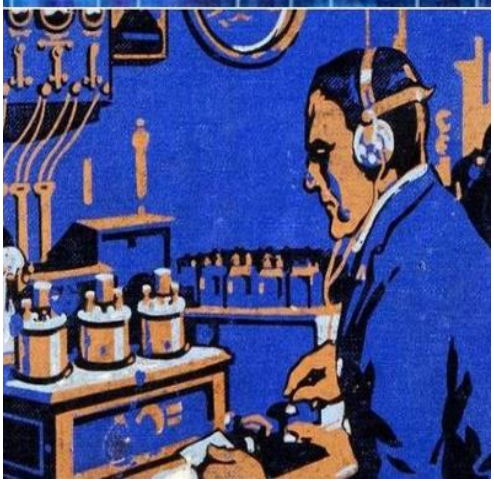
-Los números forman claves compuestas de unidades, decenas, centenas para representar letras del alfabeto o palabras comunes y nombres propios.

La época de mayor interés de la escritura cifrada española es la del Imperio español, a partir de Carlos V y durante los reinados de Felipe II, Felipe III y Felipe IV. A partir de ahí el uso de la escritura en clave iría aminorando en los manuscritos, perdiendo uniformidad en el siglo XVIII.

Recordemos de esta etapa el sistema criptográfico que las huestes de Felipe II utilizaron durante mucho tiempo utilizando un alfabeto de más de 500 símbolos que los matemáticos del rey consideraban inexpugnable. Cuando el matemático francés *François Viète* consiguió criptoanalizar aquel sistema para el rey de Francia, a la sazón Enrique IV, el conocimiento mostrado por el rey francés impulsó una queja de la corte española ante del papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos[55].

Pero, pese a los evidentes avances del criptoanálisis, aún quedan en nuestros Archivos muchos documentos de esos siglos sin descifrar.

[55] Se refiere al desciframiento por parte de François Viète del método empleado por los ejércitos de Felipe II en la guerra contra los hugonotes. En efecto, el rey español acusó a Enrique IV ante Pío V de utilizar la magia negra, y al padre del álgebra moderna de estar confabulado con el Diablo, por lo que merecía ser juzgado por el Santo Oficio. El Papa desestimó obviamente la queja, entre otras razones porque la misma curia pontificia ya venía descifrando también la correspondencia diplomática del monarca español.



MÉTODOS DE DESCIFRAMIENTO 0 CRIPTOANALÍTICOS

El desciframiento de la Criptografía se fundamenta en sucesivas inducciones y deducciones en orden al presunto significado de los textos.

Algunas normas a tener en cuenta para proceder al criptoanálisis de un documento cifrado son:

-La identificación previa de la lengua del texto.

-Hay que establecer una lista de signos empleados y fijar la frecuencia de su uso; se supone que la mayor frecuencia de una misma cifra corresponde a letras de uso más frecuente.

-Hay que fijar la atención sobre las intenciones que se tuvieron a la hora de cifrar el texto.

Colateral a estas normas es la ayuda que prestan otros conocimientos como pueden ser, entre otros, el de las fórmulas diplomáticas habituales en las cancillerías de donde procede el texto o el conocimiento de los usos frecuentes u ordinarios de redacción de los distintos países en cada época.

Conviene utilizar el método de ensayar la palabra probable, que consiste en reemplazar signos ya identificados en una palabra todavía cifrada que se presume existente en un lugar determinado.

Son indispensables, además, en esta tarea de desciframiento los manuales y repertorios cripto-gráficos y los tratados de Criptografía contemporáneos.

BIBLIOGRAFÍA

ALCOCER MARTÍNEZ, Mario: Criptografía española. Madrid, 1934.

FULLHART, Santiago Luis: Manual de Criptografía. Buenos Aires, 1945.

GALENDE DÍAZ, Juan Carlos: Criptografía. Historia de la escritura cifrada. Madrid, 1995.

"La correspondencia diplomática: Criptografía hispánica durante la Edad Moderna", en La correspondencia en la historia. Modelos y prácticas de la escritura epistolar, vol. I, Madrid, 2002.

JUHER, David: L'art de la comunicació secreta. El llenguatge de la Criptografia. Barcelona, 2004.

ORTEGA TRIGUERO, Jesús J.; LÓPEZ GUERRERO, Miguel Ángel; GARCÍA DEL CASTILLO CRESPO, Eugenio C.: Introducción a la Criptografía. Historia y actualidad. Cuenca, 2006.