La mecánica de la criptografía y su papel en la Historia

Marina Jiali Villalta Cerezo

Tutor: Servando Gutiérrez Cócera

I.E.S. Las Musas
Octubre 2018

Índice

Agradecimientos

Cuando se inicia un Proyecto de investigación, surgen muchas ideas y sueños a veces difíciles de encaminar pero que no tienen por qué desmoralizarnos. Investigar es iniciar caminos y también seguir por otras rutas antes que pararnos en el camino y retroceder.

No hay palabras para agradecer a mi tutor Servando Gutiérrez Cócera que aceptara mi trabajo y que a pesar de las dificultades me ha guiado hasta su finalización.

Con todo mi corazón doy las gracias a mi familia, que tanto me ha animado en estos seis meses a terminar mi proyecto y ante la tentación de abandonarlo, lograron que fuera no sólo completado sino que se convirtiera en motivo de orgullo para mí. He aprendido que no hay que rendirse, sino seguir siendo fiel a la idea que me atrapó cuando vi el pasado año la película *Descifrando Enigma* y estuve este verano en la avenida Alan Turing haciendo un curso propuesto por el Instituto.

Resumen

Este es un proyecto que no busca dar respuesta alguna, busca difundir y provocar en los lectores el ánimo a replantearse si de verdad sabemos qué es la criptografía y si somos conscientes del importante rol que ha tenido en el desarrollo de la Historia.

Es además un trabajo que se basa en la búsqueda de información promovida por pura curiosidad y el afán de compartir un mundo que está demasiado apartado de los libros de Historia. Nada más. Encontraremos que la criptografía es mucho más de lo que la creencia popular sostiene. Podremos apreciar la inmensa evolución que ha sufrido en el devenir histórico, estudiando los métodos que existieron desde la Antigua Grecia hasta la Segunda Guerra Mundial. No sólo veremos que ha evolucionado ella misma sino que además podremos comprender qué papel ha jugado en la Historia. Todo esto lo haremos investigando su importancia en pasajes de la Biblia, en su uso en la Política y en la Diplomacia, como también en su silenciosa labor en las hazañas bélicas.

Abstract

This is a project that does not seek to answer, it seeks to spread and provoke in readers the courage to rethink if we really know what cryptography is and if we are aware of the important role it has played in the development of History.

It is also a work based on the search of information promoted by pure curiosity and the will to share a world that we cannot find in history books. Nothing else. We will find that cryptography is much more than what popular belief holds; we will be able to appreciate the immense evolution that has undergone in the historical happening, studying the methods that existed from the Ancient Greece to the Second World War. Not only we will see that it has evolved itself, but we could also understand what role it has played in History. We will face this by investigating its importance in passages of the Bible, in its use in Diplomacy and Politics and in its silent work on military areas.

Introducción

Puede parecer de poca relevancia estudiar la criptografía "clásica" dado el inmenso avance que se ha producido en estos últimos años, pero han sido las siguientes razones las que nos instan a estudiarla. La primera es el valor histórico que tiene, el ser capaces de comprender documentos encriptados en aquellas épocas aporta mucho a la ciencia historiográfica. Y la segunda es algo evidente, se siguen utilizando los encriptados de "lápiz y papel" en muchos casos similares a los que ya se dieron en la Historia. Por lo que no sólo su importancia es histórica sino que actualmente sigue siendo algo cotidiano.

Hemos abordado los métodos más importantes que se han dado en el devenir histórico así como la mecánica de los mismos. La Biblia, la Diplomacia, la Política y las hazañas bélicas han sido los cuatro campos que han centrado nuestro interés. En todas ellas la criptografía ha dejado una huella que hemos querido divulgar en este trabajo.

Queremos otorgar en este trabajo espacio a España, un país donde la evolución de la criptografía brilló por sus altibajos. Si en tiempos de Fernando el Católico y Felipe II destacábamos por ser pioneros, hasta la Guerra Civil Española se ha dado un estancamiento de la misma.

Mientras Europa fue escenario de grandes avances que dieron a conocer figuras como Alberti en Italia, Rossignol y Vigenère en Francia. Los ingleses con Bletchley Park marcarían una nueva era con el criptoanálisis de la máquina Enigma, sentando las bases de la Ciberseguridad actual.

Tema de estudio

Este proyecto de investigación gira en torno a las siguientes preguntas:

¿Sabemos qué es y cómo funciona la criptografía?

¿Hasta qué punto ha repercutido la criptografía en la Historia?

Hipótesis inicial

La criptografía es el conjunto de métodos que se han ido creando a lo largo del tiempo para proteger información vital cuando era enviada de un lugar a otro. Su funcionamiento consiste en crear, a raíz del mensaje, un texto ilegible siguiendo un patrón que modifica al original.

Sólo con conocer el caso de Enigma y el papel que desempeñó en la Segunda Guerra Mundial, sabemos que la criptografía ha repercutido en gran medida en la Historia. De hecho, hoy en día espionaje y Ciberseguridad son dos campos de suma importancia en la defensa de los países y de las empresas cuyo precedente común ha sido la criptografía.

Capítulo I: La esteganografía y la criptografía

Esteganografía: la escritura secreta

El tema nos obliga, sin duda alguna, a comenzar por el principio de todo: la esteganografía. Esta se conoce como el arte o ciencia de comunicar de manera oculta un mensaje, camuflando dicha información entre otro conjunto de datos para que pase desapercibida. Proviene del griego *steganos* (secreto) y *grafos* (escrito). Para conocer sus primeros pasos nos tenemos que remontar al siglo V a. C. en la Antigua Grecia con Herodoto de Halicarnaso (484 – 425 a.C.)

En *Las historias* sobre las Guerras Médicas, Herodoto revela cómo el rey persa Jerjes planeaba un ataque sorpresa a los griegos. Demarato, un fugitivo espartano, enterado de los planes de asalto del rey, quiso avisar a los griegos. Pero no podía permitir que los persas se enteraran de ello, e ideó un procedimiento para ocultar el mensaje. El método consistió en coger un cuadernillo de dos tablillas, quitar la cera que cubría la madera y sobre la misma, grabar el mensaje; después volver a aplicar una capa de cera ocultando así el escrito, de forma que "el portador de un cuadernillo en blanco no fuera molestado de los guardas de los caminos". Una vez llegada la tablilla al poder de los griegos, estos sólo tuvieron que retirar la cera y así accedieron al comunicado oculto.[1]

Otro ejemplo que también se relata en *Las Historias*, se da con Histieo, un general ateniense que había ganado el control de Mileto en el 499 a. C. como premio dado por el persa Darío I, ya que le salvó de una contienda contra los escitas. Este le otorgó también el título de "compañero de la mesa real" lo que hizo que Histieo tuviera que abandonar su patria para ir hasta Susa. Pasado un tiempo y con el afán de recuperar su poder en Mileto, Histieo escogió a su mejor esclavo, le afeitó la cabeza, le tatuó en ella un mensaje. Esperó a que le volviera a crecer el cabello y le envió a Aristágonas, yerno suyo, quien era tirano interino en Mileto. Allí, Aristágonas sólo tuvo que afeitarle de nuevo para saber el contenido del mensaje. Este le instaba a que se levantara contra los persas. Aristágonas, siguió las indicaciones y desató así la Revuelta de Jonia, el primer gran conflicto entre persas y griegos.

Si nos acercamos a la Edad Media, sabemos que proliferaron los mensajes escritos con la famosa "tinta invisible" que mencionó el escritor y científico latino Plinio el Viejo en el siglo I d.C. Consistía en usar la savia de la planta Tithymallus que se volvía transparente al secarse, pero se chamuscaba si la calentabas y se volvía marrón. También se usaron los famosos jugos de limón o cebolla exprimidos, que bajo el calor de la vela aparecía el mensaje oculto. Este viejo método llegó hasta el

[1] Herodoto *Los nueve Libros de la Historia* Libro VII. Recuperado en : http://www.enxarxa.com/biblioteca/HERODOTO%20Historia%20_Pou_.pdf

siglo XIX en España, puesto que en la Primera Guerra Carlista (1833-39) el general Zumalacárregui y Don Carlos de Borbón, que reclamaba el trono de Fernando VII, lo utilizaban para comunicarse.

Avanzando en la línea del tiempo, exactamente hasta la Segunda Guerra Mundial, descubrimos que se usaron los llamados "microfilmes" que escondían en los puntos de las íes o signos de puntuación, micro-mensajes en código morse. Otro cifrado que se usó fue el llamado "Null Cipher" que consistía en enviar un mensaje trivial y en una parte del mismo ocultar el texto. Hay muchas maneras de usar el "Null Cipher", por ejemplo, cogiendo la primera letra de cada palabra del texto.

Texto encriptado	**H**a **o**lido **y**a **a**l toro **a**tado **c**on **a**rnés **d**orado.
Mensaje desencriptado	Hoy atacad

Figura 1

Siendo esta la era digital, la tecnología también ha tenido una evolución vertiginosa. Ahora podemos ocultar información en todo tipo de archivos, imágenes, vídeos…

Criptografía

La propia palabra proviene del griego *kryptos*, que significa "ocultar" y *grafos* "escrito"; es decir, "escritura oculta". Con ello podemos definir a la criptografía como el conjunto de técnicas empleadas en proteger datos de forma que se establezca una comunicación segura y dichos datos solo puedan ser leídos por aquellos a quienes van dirigidos.

Existen dos términos que se usarán a lo largo de este trabajo de investigación:

- *Plaintext* o texto llano: el texto a encriptar
- *Ciphertext*: el texto ya encriptado

Distinguimos 2 tipos de transformaciones:

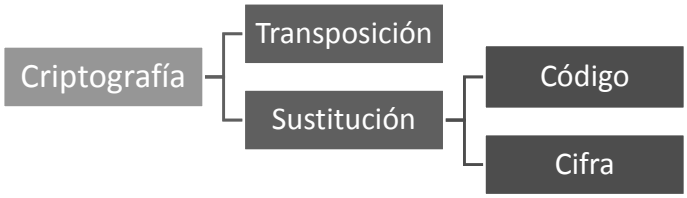


Figura 2

La **Transposición**, la más simple, cambia el orden de las letras del texto a encriptar.

Este es el procedimiento:

1. Se escoge una clave, cada letra se colocará en una columna, se enumerarán por orden alfabético y si alguna letra se repitiera, su orden sería de izquierda a derecha.
2. El texto a encriptar se escribe horizontalmente en filas.
3. El texto cifrado se leerá por columnas siguiendo el orden de las letras de la palabra clave.

Por ejemplo:

- Texto a encriptar: *Inminente ataque de los griegos*
- Clave: Herodoto

H	E	R	O	D	O	T	O
3	2	7	4	1	5	8	6
I	N	M	I	N	E	N	T
E	A	T	A	Q	U	E	D
E	L	O	S	G	R	I	E
G	O	S					

Figura 3

- El texto cifrado resultaría así: **NQG NALO IEEG IAS EUE TDS MTOS NER**

Para desencriptarlo, se sigue el mismo procedimiento; se coloca la clave, la enumeramos como ha sido acordado y escribimos las letras en el correspondiente orden.

Seguidamente, en la **Sustitución**, como su propio nombre indica, las letras son cambiadas por otras o símbolos o números. Es un sistema mucho más importante y diverso que la Transposición. Se apoya en los alfabetos de cifrado (*cipheralphabet*), que son las listas de equivalentes que se usan para transformar el texto a cifrar en un texto cifrado. Un ejemplo simple de un alfabeto de cifrado puede ser el siguiente:

Letras del texto a encriptar	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
Letras del texto cifrado	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F
Letras del texto a encriptar	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
Letras del texto cifrado	G	H	J	K	L	Ñ	Z	X	C	V	B	N	M	

Figura 4

Siguiendo este alfabeto, la palabra *enemigo* sería: **tftdouh**

A veces hay algunos alfabetos, que, para despistar al adversario incluyen símbolos que no significan nada. Se llaman "**nulls**" o **nulos**. También puede ocurrir que un alfabeto dé varias opciones de sustitución a una única letra; estas opciones se llaman "**homophones**" u **homófonos**.

Si un texto sólo sigue un alfabeto, como en el ejemplo anterior, se llama un sistema **monoalfabético**. En cambio, si se somete al texto a dos o más alfabetos de cifrado, este sistema

se convierte en **polialfabético**. Actualmente las máquinas modernas de cifrados emplean millones de *cipheralphabet*.

Como vemos en Figura 1, dentro de los cifrados por Sustitución distinguimos el código de la cifra. La diferencia es simple, el código consiste en una lista de miles de palabras, frases y sílabas con su correspondiente clave que los reemplaza al cifrar el texto. Es decir, para cada palabra, sílaba o frase existe lo que se llama un *codeword* o *codenumber* según si son palabras o números. Un código puede ser de dos tipos:

- "One-part code": las palabras a encriptar están en orden ya sea alfabético o numérico. Por ello un único libro es suficiente para codificar y decodificar un texto.

Palabra del texto a encriptar	Código
Irremediable	HVBA
Irremisible	HVBB
Irreparable	HVBC
Irrepetible	HVBD
Irreprensible	HVBE

Figura 5

- "Two-part code": Solo una de las columnas está ordenada. Por una parte, las palabras del texto a encriptar ordenadas alfabéticamente pero el código no (Figura 6) y por otra parte, el código ordenado pero no las palabras del texto a encriptar (Figura 7). Para decodificar el texto es necesario los dos libros.

Palabra del texto a encriptar	Código
Politología	15003
Políticólogo	50987
Politraumatismo	45698
Poliuretano	21587
Poliura	67902

Figura 6

Palabra del texto a encriptar	Código
Grecia	10001
Ataque	10002
Mañana	10003
Flecha	10004
Persia	10005

Figura 7

Vemos entonces, que un código crea un gigantesco alfabeto de cifrado donde las palabras y las frases clave son dotadas de un código correspondiente. También se añaden sílabas y letras de

forma que, si fuera necesario escribir alguna palabra que no se encontrara en el código, se pudiera realizar el cifrado. Por lo tanto, la unidad básica del código son palabras y frases. En cambio, en la cifra, la unidad básica son las letras, a veces pares de letras (**bigram**) y aunque es muy poco común, grupos de letras (**poligram**).

La primera diferencia es evidente, la unidad básica del código son las palabras y frases y la unidad básica de la cifra son las letras; pero la diferencia más notoria entre ambos es que el código está atado a las reglas del idioma, pues lo que codifica son elementos con significado (palabras y frases) mientras que la cifra sólo convierte letras.

Se llamó **Nomenclator** a un pequeño libro de códigos con una gran tabla de homófonos de palabras, nombres clave y sílabas. En un principio consistía sólo en listas de nombres, de ahí Nomenclator. La familia francesa **Rossignol** creó "The Great Cypher" un claro ejemplo de Nomenclator, usado por Luis XIV "El Rey Sol" de Francia; fue una revolución en aquella época, donde se seguían usando los básicos y fáciles cifrados monoalfabéticos. Esta "Gran Cifra" no sólo sustituía letras, también sílabas y números; de esta forma era imposible usar el Método del Análisis de Frecuencia[2]. Además el cifrado ignoraba la sílaba o letra precedente, haciendo aún más complicado su descifrado y el hecho de averiguar qué era una parte del cifrado y qué un sinsentido.

La gran mayoría de los cifrados usan una llave (key) con la que se especifican datos del cifrado, tales como el orden de las letras, el patrón de sustitución o los ajustes de una máquina de cifrado. Si dicha clave fuera una palabra, frase o número se llamaría "keyword", "keyphrase" o "keynumber" respectivamente.

Ciclo de la criptografía

Llamamos **encriptar** o **codificar** a hacer pasar un "plaintext" o texto llano, por las ya mencionadas transformaciones. La resultante de las mismas es el "ciphertext" o "codetext" según el método utilizado: la cifra o el código. Una vez protegido el "plaintext" se envía y se convierte en lo que llamamos **criptograma;** la diferencia entre "ciphertext" y criptograma reside en que el "ciphertext" hace más énfasis en el propio encriptado y el criptograma en su transmisión, lo que sería un análogo del telegrama.

[2] Creado por el árabe Al-Kindi analizaba todo un texto no cifrado y recogía una tabla con las frecuencias de cada letra. Después, ya con el texto encriptado, volvía a diseñar una nueva tabla de frecuencia con las nuevas letras y las iba comparando. La letra de mayor frecuencia del primer texto, se correspondía entonces con la letra de mayor frecuencia del segundo. Ver también el Capítulo IV de este trabajo

Por otra parte **desencriptar** o **decodificar** es un término reservado a los destinatarios del mensaje encriptado, aquellos que tienen la *key* y por tanto pueden revertir las transformaciones del "ciphertext" para obtener el mensaje original. El "enemigo" que no tiene la llave pero quiere acceder al texto debe de realizar el Criptoanálisis o el "codebreaking" para así quitar la protección del mismo y obtener el "*plaintext*". También reciben un nombre los mensajes que no han sido protegidos. Se llaman "cleartext". La siguiente figura retrata el ciclo descrito.

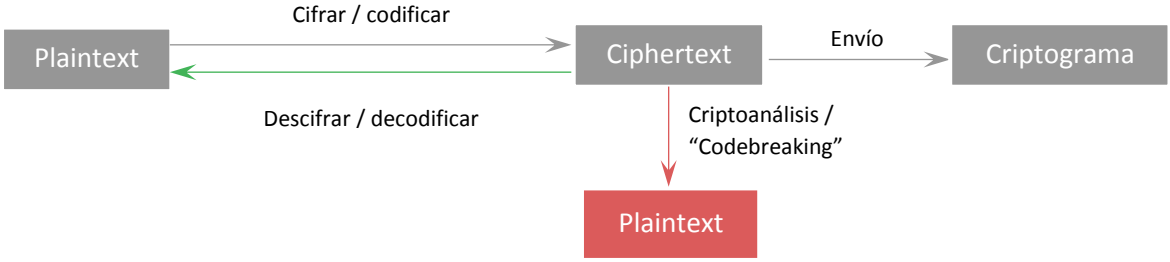


Figura 8. Para poder proteger un mensaje el emisor lo que hace es codificarlo o cifrarlo, convirtiendo el Plaintext en un Ciphertext. Una vez enviado al receptor pasará de Ciphertext a llamarse Criptograma. El receptor del mensaje, que tiene en su poder la key del cifrado, la usará para descifrar o decodificar el ciphertext para conseguir el mensaje original (marcado en verde). Si el ciphertext fuera interceptado por un usuario no deseado, para poder descifrarlo el "enemigo" deberá de hacer su correspondiente Criptoanálisis o "Codebreaking" consiguiendo así el mensaje original (marcado en rojo).

Todo esto ha sido recopilado en la ciencia de la **Criptología**, que no sólo abarca la criptografía sino también el criptoanálisis, es decir, la protección de información y la extracción de la misma.

PROTECCIÓN **SIGNAL SECURITY**	**SUSTRACCIÓN** **SIGNAL INTELLIGENCE**
Communication Security Steganography (invisible inks, open codes, messages in hollow heles) and Transmission Security (spurt radio system)	Communication Intelligence Intercepting and Direction-Finding
Transmission Security (call-sign changes, dummy messages	Traffic Analysis (direction-finding fixes, messages-flow studies, radio-fingerprinting)
Cryptography (codes and ciphers, ciphony, cifax)	Cryptanalysis
Electronic Security Emission Security (shifting of radar frequencies)	Electronic Intelligence Electronic Reconnaissance (eavesdropping on radar emissions)
Counter-Countermeasures ("looking-through" jammed radar)	Countermeasures (jamming, false radar echoes)

Figura 9[3]

[3] Kahn, D. (1967), *The codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*

Capítulo II: Métodos y mecánica de la criptografía

La Escítala espartana

El primer uso de criptografía en el campo militar es del siglo V a. C. cuando los espartanos emplearon la escítala para encriptar sus mensajes en las guerras entre Atenas y Esparta (Guerras del Peloponeso).

Esta es una vara de madera a la que se le enrolla una larga tira de tela, papel o pergamino, tal y como se muestra en la Figura 10. El emisor escribe el mensaje horizontalmente a lo largo de la vara y después la desenrolla pareciendo esta una larga lista de letras y números sin sentido alguno. Una vez enviado el receptor, que tiene en su poder una vara del mismo diámetro enrosca la tira de nuevo y recupera el mensaje encriptado. La referencia de este método la encontramos en el tercer tomo de *Vidas Paralelas* de Plutarco del siglo II d. C.

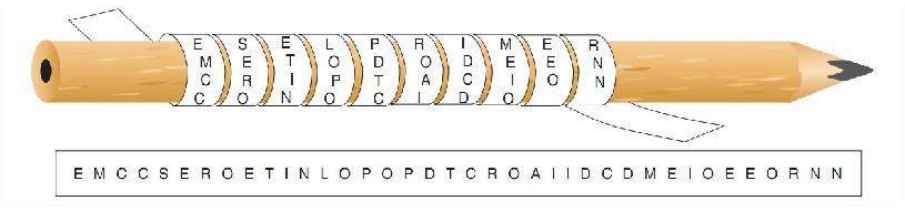


Figura 10[4]

Para comprenderla mejor imaginemos un mensaje compuesto por 4 filas de 10 caracteres de longitud (como en la Figura) cuando la desenrollamos obtenemos una tira con 36 letras, donde la primera letra es la primera letra de la primera línea; la segunda será la primera letra de la segunda línea y así hasta la cuarta letra. La quinta letra es la segunda letra de la primera fila y así hasta el final. De esta forma y para esta combinación de **n** filas podemos afirmar que la **j**-ésima letra de la **i**-ésima fila ocupará el lugar:

$$n(j-1)+i$$

Por ejemplo, si cogemos de la Figura 10 la cuarta letra de la segunda fila (O), en la tira desenrollada ocupará la posición número 14.

Este es un método de criptografía de transposición, pues lo que realmente se ha hecho ha sido una desordenación de los caracteres del mensaje. Su criptoanálisis es sencillo, se parte de la primera letra y se va tomando letras dando saltos de 2 letras; si se obtuviera un mensaje con sentido, la escítala solo tendría 2 filas, si no fuera el caso, se repetiría el proceso pero dando saltos de 3 letras. Así hasta que se obtuviera el mensaje completo.

[4] Ilustración Escítala espartana. Recuperado de https://ciclosistemasmicroinformaticosjorgemilenablog.files.wordpress.com/2015/12/1.png

El cifrado de Polibio

Inventado por el historiador griego Polibio (200-118 a. C). Este es un método de cifrado de sustitución, y consistía en sustituir una letra con su correspondiente fila y columna en "El cuadrado de Polibio"

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

Figura 11[5]

La letra "A" se cifrará como 11, la "B" como 12 y así correspondiéndose la primera letra con la fila y la segunda con la columna. Un ejemplo de su uso sería:

◊ Texto a encriptar: *Ataque al amanecer*

◊ Texto encriptado: **114411414515 1131 1132113315131542**

La principal ventaja que tenía este cifrado era su simplicidad, pues reducía el alfabeto a 5 únicas letras, pero con un problema porque hacía el mensaje el doble de largo que el original.

Un claro sucesor de este método es Francis Bacon, filósofo inglés del siglo XVI (Véase Anexo I). Su mecánica era asociar a cada letra del alfabeto una secuencia de 5 letras, siendo únicamente la A y la B. Y creó esta cifra:

A	AAAAA	G	AABBA	N	ABBAA	T	BAABA
B	AAAAB	H	AABBB	O	ABBAB	U-V	BAABB
C	AAABA	I-J	ABAAA	P	ABBBA	W	BABAA
D	AAABB	K	ABAAB	Q	ABBBB	X	BABAB
E	AABAA	L	ABABA	R	BAAAA	Y	BABBA
F	AABAB	M	ABABB	S	BAAAB	Z	BABBB

Figura 12[6]

Por ejemplo:

◊ Texto a encriptar: *Ataque al amanecer*

◊ Texto encriptado: **AAAAABAABAAAAAAABBBBBAABBAABAA AAAAAABABA AAAAAABABBAAAAAABBAAAABAAAAABAAABAABAAAA**

[5] *Códigos secretos en la Primera Guerra Mundial* (11-3-2015), Cuaderno de Cultura Científica. Recuperado de: https://culturacientifica.com/2015/03/11/codigos-secretos-en-la-primera-guerra-mundial/

[6] Bacon, F. (1605). *El avance del saber*, Inglaterra.

Como se daba en el cifrado de Polibio aquí también sucede, la extensión del texto encriptado es inmensa y es muy costoso encriptar pues hace el *plaintext* cinco veces más extenso.

El *atbash* hebreo

Es un método que aparece en la Biblia, un cifrado monoalfabético de sustitución, es decir, modifica las letras del mensaje por otras. Su mecánica consistía en cambiar la primera letra del alfabeto hebreo o *alefato* con la última, la segunda con la penúltima y así sucesivamente.

Normal:	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Inverso:	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Figura 13[7]

En español resultaría así:

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

Figura 14

De forma que:

- Texto a encriptar: *Yahveh*
- Texto encriptado: **BZSEVS**

Este es un cifrado que destaca por su simpleza y, por tanto, por su vulnerabilidad ante los criptoanálisis.

El cifrado de César

Como su propio nombre indica, fue usado en tiempos de la Roma Imperial, por Julio César (100-44 a.C.). Un cifrado monoalfabético de sustitución, donde, escogía una letra y la cambiaba por una tres posiciones más allá en el alfabeto, de forma que la A se convertía en D, la B en E y así hasta que la Z se convirtiera en C.

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

Figura 15

Aunque el historiador Suetonio (siglo I) sólo mencionara un desplazamiento de 3 posiciones, es evidente que usando cualquier cambio entre 1 y 25 lugares puede generar 25 cifras diferentes.

[7] *Criptografía en la Biblia* (5-8-2014). KORANET. Extraído de: https://koranets.net/criptografia-en-la-biblia/

Simon Singh (2000) afirmaba que, si no se limitaran a cambiar ordenadamente el alfabeto pudiendo hacer cualquier combinación del *plaintext* se podría generar un número aún mayor de cifras distintas.

"Hay más de 400.000.000.000.000.000.000.000.000 combinaciones posibles y, por tanto, de cifras diferentes" [8].

Un ejemplo de este cifrado sería:

◊ Texto a encriptar: *Ave Cesar*

◊ Texto encriptado: **DYH FHVDU**

Como en la escítala, podemos llegar a una fórmula general para este cifrado. Para ello debemos asignar a cada letra un número (A = 00, B = 01, C = 02,...Z = 25) y considerando un alfabeto de 26 letras llegamos a esta fórmula[9]:

$$C \equiv (M + 3)(mód\ 26)$$

Donde M corresponde a la letra del *plaintext* y C la correspondiente a M cifrada.

El alfabeto de 26 letras y sus valores asignados sería, por ejemplo este:

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

Figura 16

Por ejemplo, si escogemos la letra Q con valor 16 y realizamos la operación:

$$C = (16 + 3)(mód\ 26) = 19$$

Miramos en la tabla la letra que corresponde al 19, la T. Y sustituimos la Q por T.

El cifrado de Leon Alberti

Creado en 1466 por el científico, teórico y artista italiano del Renacimiento Leon Battista Alberti (1404-1472) quien propuso un nuevo e innovador método criptográfico al que llamamos Disco de Alberti. En su tratado *De Componendis Cyphris* explica:

"Hago dos discos con dos láminas de cobre. Uno, el mayor, será fijo y el otro móvil. El diámetro del disco fijo será superior en un noveno al disco móvil. Divido la circunferencia de los discos en 24 partes iguales llamadas sectores. En cada uno de los sectores del disco grande escribo en orden alfabético normal una letra mayúscula roja: primero la A, seguida de la B, después la C, etc., omitiendo H y K que no son indispensables."

[8] Singh, S, (2000), *The code book: Science of Secrecy*, Debate

[9] Fernández, S (2004). La criptografía clásica. *Sigma, (24)*

Como en el latín no existen las letras J, U W e Y, rellena 20 sectores y deja libres 4 para rellenarlos con los números del 1 al 4. Continúa contando cómo rellenará el disco pequeño.

"... una letra minúscula, pero no en su orden normal como en el disco fijo, sino en un orden incoherente. De esta forma se puede suponerse que la primera letra será la a, la segunda la g, tercera la q y así hasta rellenar los 24 sectores, porque el alfabeto latino consta de 24 caracteres, siendo el vigesimocuarto et. Efectuadas estas operaciones, se coloca el disco pequeño sobre el grande de modo que una aguja pasada por los dos centros sirva como eje común alrededor del cual girará el disco móvil."

Ahora que los discos giran sobre un mismo eje, escogemos una letra a cifrar, por ejemplo, la K. En el disco pequeño localizamos dicha letra y la alineamos con cualquiera de las letras del disco más grande, por ejemplo, la B y notifica al receptor del mensaje de esta alineación.

"... Usando este punto de partida, cada letra del mensaje representará a la letra fija que hay sobre ella. Después de escribir tres o cuatro letras, puedo cambiar la posición de la letra clave de modo que la k esté, por ejemplo, sobre la D. Después en mi mensaje escribo una D mayúscula y, a partir de este punto, k ya no significará B y si D, y todas la letras del disco fijo tienen nuevas identidades."

Esto significa que, por cada giro que dé la rueda superior, el alfabeto de cifrado cambiará haciéndolo polialfabético. Además se notificará al receptor del correspondiente giro escribiendo con mayúscula el nuevo valor de la letra clave. Para verlo más claro veamos un ejemplo alineando la *k*.

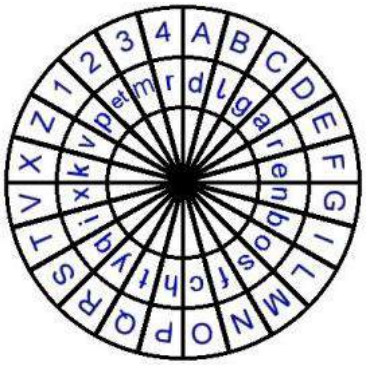


Figura 17[10]

- Texto a encriptar: *LEONBATTISTAALBERTI*
- Texto encriptado: **XorcfAvkfflfkNoishmdq**

[10] Tabara Carbajo, J. L. (s.f.). *Criptografía clásica.* GitBooks. Recuperado de https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto11.html

La rejilla de Cardano

Un método de cifrado inventado hacia 1550 por el matemático italiano Gerolamo Cardano (1501-1576). Era un cifrado monoalfabético de transposición que precisaba, como su nombre indica, de una rejilla idéntica en poder de emisor y receptor lo que restaba seguridad pues podía ser robado, duplicado o incluso cambiado, debido a la facilidad que tenía de ser producida.

El método era simple, una rejilla que contenía en cada uno de sus agujeros el número en el que han de colocarse las letras del mensaje. Por ejemplo: queremos cifrar "*Inminente emboscada*" de 18 letras y tenemos la siguiente tablilla:

1	12	14	5
3	18	7	16
6	10	8	13
17	15	4	11
9	2		

1. Colocamos las letras en el orden que dicta la tablilla:

I	M	S	N
M	A	N	A
E	E	T	O
D	C	I	M
E	N		

2. Quedando el ciphertext así: **IMSNMANAEETODCIMEN**
3. El receptor tendría que colocar el mensaje cifrado en su tablilla y obtendrá el mensaje original.

Cifrado de Vigenère

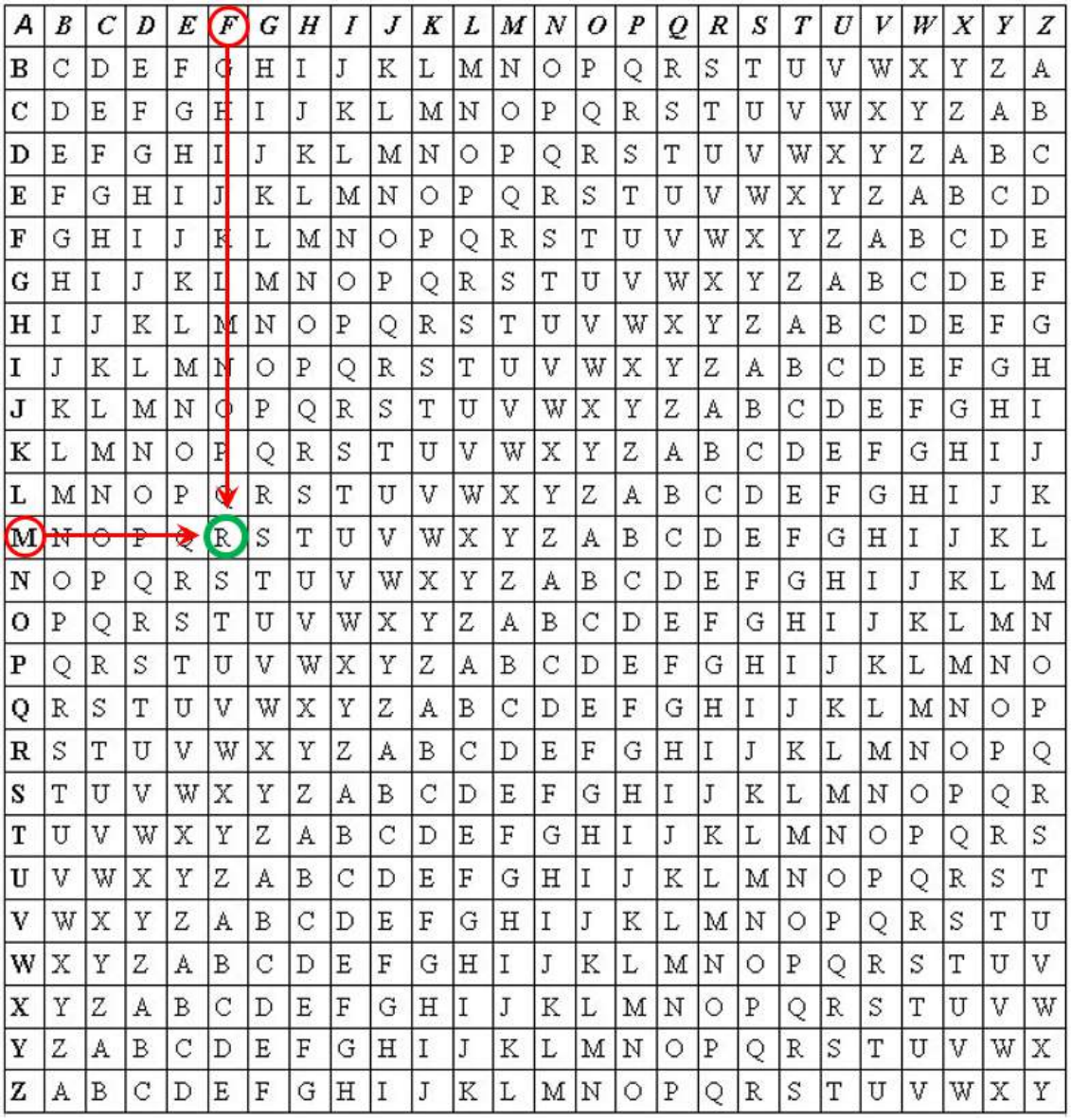
El nombre del criptógrafo francés Blaise de Vigenère (1523-1597) se asocia, aunque erróneamente [11], a uno de los métodos más famosos de la criptografía de sustitución polialfabética y que describió por primera vez en 1586.

El "Tablero de Vigenère" es una disposición de los 26 alfabetos de César (de 26 letras), donde se introduce una clave (palabra o texto) que se repite a lo largo de todo el mensaje a cifrar para después buscar su equivalente alfabeto César que comience con dicha letra.

[11] Este método fue antes descrito en 1553 por otro criptólogo muy famoso de la época llamado Giovan Battista Bellaso en su libro *La cifra del Sig. Giovan Battista Belasso.*

Su procedimiento es el siguiente:

1. Se acuerda una clave
2. Se repite la clave debajo del texto tantas veces sea necesario
3. Cada letra del *plaintext* se localizará en la primera columna de letras y cada letra correspondiente de la clave, se localizará en la primera fila.
4. La letra de la fila marcada por la letra del *plaintext* y de la columna marcada por la clave será la letra del ciphertext.



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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Figura 18[12]

[12] Recuperado de https://de.wikipedia.org/wiki/Datei:VigenereSquare2.jpg

Por ejemplo:

- Clave: flecha
- Texto a encriptar: *Muerte premeditada*

Texto a encriptar	M	U	E	R	T	E	P	R	E	M	E	D	I	T	A	D	A
Clave	F	L	E	C	H	A	F	L	E	C	H	A	F	L	E	C	H

Figura 19

Para la primera letra del texto a encriptar nos fijamos en la Figura 18, la M se convertirá en una R. De esta forma obtenemos el texto cifrado que será: **RFITAE UCIOLDNEEFH**

La cifra ADFGVX

Cifrado introducido por primera vez el 5 de marzo de 1918 cuando los alemanes iban a lanzar una ofensiva en la Primera Guerra Mundial. La principal característica del método residía en que era uno de los primeros que unían transposición con sustitución.

La mecánica consistía en dibujar una cuadrícula de 7x7 donde colocamos en la primera fila y en la primera columna las letras: A, D, F, G, V y X. Los 36 cuadrados interiores se completan aleatoriamente con el alfabeto y las 10 cifras.

Por ejemplo con esta disposición:

	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

Figura 20[13]

Siguiendo esta tabla, por ejemplo el número 3 cifrado será VG.

- Texto a encriptar: *Apoyo aéreo*
- Texto encriptado: **GXGVXGVAXG GXVVFVVVXG**

Hasta este punto no deja de ser un cifrado de sustitución convencional. En la segunda fase el texto pasará una transposición. Escogemos una clave o key que sea una única palabra, en este

[13] *El cifrado ADFGVX* [Tabla modelo de cifrado ADFGVX] Recuperado de http://paraisomat.ii.uned.es/paraiso/cripto.php?id=adfgvx

caso ARCOS y la colocamos en una tabla en la primera fila letra a letra. Debajo de esta escribimos columna a columna el texto encriptado de la fase 1.

A	R	C	O	S
G	X	G	V	X
G	V	A	X	G
G	X	V	V	F
V	V	V	X	G

Si faltaran por rellenar huecos se añadirían caracteres de relleno. Ahora se cambiarían de posición las columnas de forma que las letras de la clave esté en orden alfabético.

A	C	O	R	S
G	G	V	X	X
G	A	X	V	G
G	V	V	X	F
V	V	X	V	G

Leemos ahora el texto resultante que será: **GGVXXGAXVGGVVXFVVXVG**

Por último, se traduce el texto al Morse pues í era como se transmitía, quedando finalmente así: **--. --. ...- -..- -..- --. .- -..- ...- --. --. ...- ...- -..- ..-. ...- ...- -..- ...- --. .-.-.**

La máquina Enigma

En 1918 el inventor alemán Arthur Scherbius y Richard Ritter investigaron formas de sustituir los inadecuados sistemas criptográficos que se usaron en la Primera Guerra Mundial basados en una cifra de "lápiz y papel"[14]. Con sus conocimientos de ingeniería eléctrica desarrollaron una pieza de maquinaria criptográfica que era una versión eléctrica del Disco de Alberti. Este sería el más temible sistema de codificación de la Historia al que llamaron Enigma.

[14] Singh, S, (2000), *The code book: Science of Secrecy* (p. 148). Ed. Debate

Podíamos dividir la máquina en 3 partes que estaban interconectadas: un teclado donde se escribía el texto a cifrar, una unidad modificadora que codificaba cada letra del *plaintext* en la correspondiente letra de texto cifrado y un tablero expositor de varias lámparas para indicar la letra codificada.

El modificador, es un disco plagado de cables, es la parte más importante de la máquina.

"Desde el teclado, los cables entran en el modificador por seis puntos y luego hacen una serie de giros y rodeos dentro del modificador antes de salir por seis puntos al otro lado. El cableado interno del modificador determina cómo serán codificadas las letras del texto llano."[15]

Siguiendo la Figura 21 el cableado nos indica que: Si pulsamos la tecla a iluminará la B, pulsando la tecla b iluminará la letra **A,** la tecla c iluminará la letra **D,** la tecla d iluminará la letra **F**, la tecla e iluminará la letra **E** y pulsando la tecla f iluminará la letra **C**

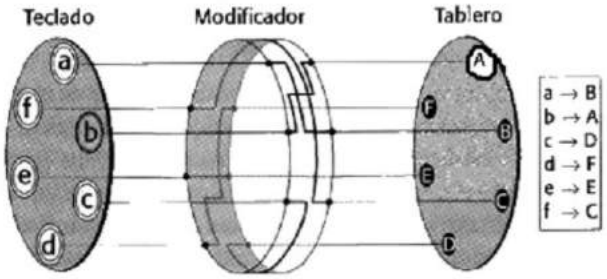


Figura 21[16]*. Una versión simplificada de la máquina Enigma con un alfabeto de únicamente 6 letras. Distinguimos los cables que van desde el teclado, pasando por el modificador para terminar en el tablero. Al pulsar la tecla A la corriente va a través del cable e ilumina la letra B del tablero. El recuadro a la derecha es la codificación de cada una de las letras.*

Pero este cifrado no deja de ser una simple cifra monoalfabética fácil de descubrir, por lo que Scherbius colocó una segunda unidad modificadora e hizo que la primera unidad girara cada vez que se pulsara una posición. Y cuando éste diera una vuelta completa el segundo disco giraría también una posición (ver Figura 22). Añadiendo un modificador más, lográbamos pasar de una clave de 26 posiciones a una clave de 676 e incluso, más tarde, se añadió un tercer disco que, como hacía el segundo con el primero, cuando el segundo daba una vuelta completa éste avanzaba una posición, logrando una cantidad total de 17.576 posiciones posibles.

Un complemento más que tenía Enigma era el reflector, dispositivo diseñado exclusivamente para el desencriptado de los mensajes. Una vez llegado al destino el criptograma se tecleaba en otra máquina Enigma dispuesta de la misma forma que la tenían los emisores y a través del receptor, se reproducía el mensaje original.

[15] *Ibídem* (p. 149)
[16] Singh, S, (2000), *The code book: Science of Secrecy* (p. 150). Ed. Debate

Las posiciones iniciales de la máquina eran la clave de todo el encriptado. Generalmente las posiciones iniciales vendrían dictadas por un libro de códigos que contendría una clave para cada día, pero los alemanes descartaron esta opción por lo complejo y tedioso que era este método y optaron por enviar cada cuatro semanas un libro de 28 claves, una para cada día.

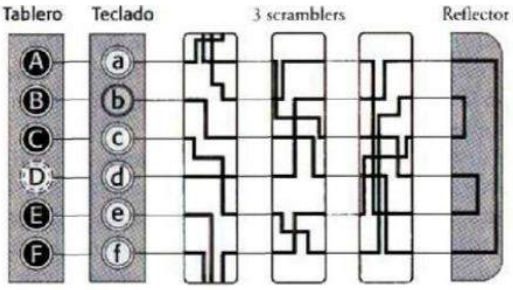


Figura 22[17]

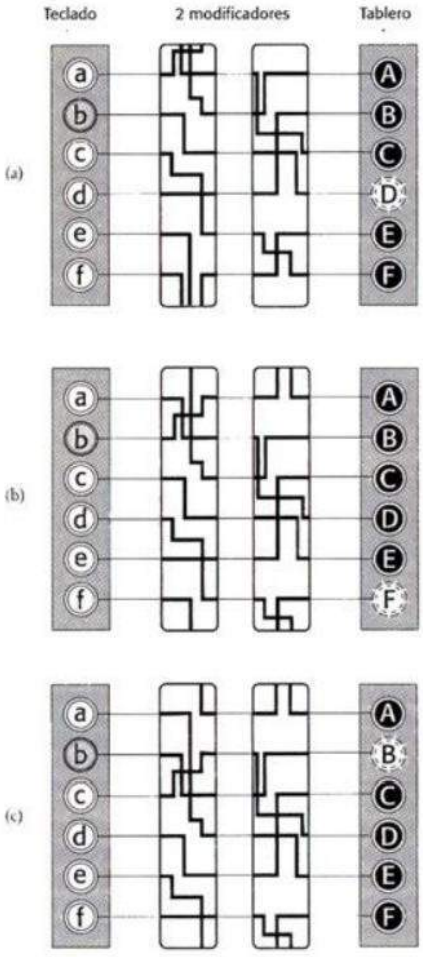


Figura 23. "Al añadir un segundo modificador, el patrón de codificación no se repite hasta que se han codificado 36 letras, y ambos modificadores han vuelto a sus posiciones originales. Para simplificar el diagrama, los modificadores están representados en dos dimensiones: en vez de girar una posición, los cableados descienden una posición. Si un cable parece dejar la parte superior o interior de un modificador, su sendero se puede seguir continuando desde el cable correspondiente de la parte inferior o superior del mismo modificador, en (a), b se codifica como D. Después de la codificación, el primer modificador gira una posición, haciendo que también el segundo modificador se mueva una posición —esto sucede sólo una vez durante cada revolución completa de la primera rueda—. Esta nueva disposición se muestra en (b), en la que b se codifica como F. Después de la codificación, el primer modificador gira una posición, pero esta vez el Figura 18. "Al añadir un segundo modificador, el patrón de codificación no se repite hasta que se han codificado 36 letras, y ambos modificadores han vuelto a sus posiciones originales. Para simplificar el diagrama, los modificadores están representados en dos dimensiones: en vez de girar una posición, los cableados descienden una posición. Si un cable parece dejar la parte superior o interior de un modificador, su sendero se puede seguir continuando desde el cable correspondiente de la parte inferior o superior del mismo modificador, en (a), b se codifica como D. Después de la codificación, el primer modificador gira una posición, haciendo que también el segundo modificador se mueva una posición —esto sucede sólo una vez durante cada revolución completa de la primera rueda—. Esta nueva disposición se muestra en (b), en la que b se codifica como F. Después de la codificación, el primer modificador gira una posición, pero esta vez el segundo modificador permanece fijo. Esta nueva disposición se muestra en (c) en la que b se codifica como B." [18]

[17] Singh, S, (2000), *The code book: Science of Secrecy* (p. 152). Ed. Debate
[18] *Ibídem (p. 155)*

Pero el avance no se detuvo ahí, Scherbius añadiría 2 nuevas características:

- Los rotores serían intercambiables aumentando así la cantidad de claves posibles.
- Se introdujo un clavijero con el que se podrían intercambiar pares de letras en grupos de 6

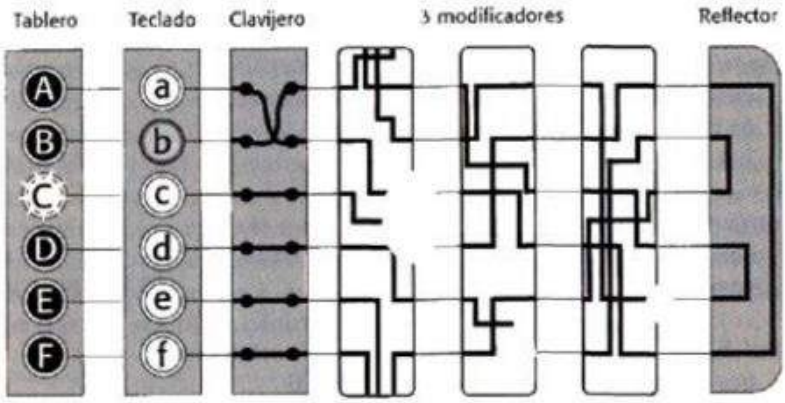


Figura 24. Podemos observar como la adición del clavijero altera el orden de "a" y "b" al intercambiarlas. En la Enigma real habría posibilidad de intercambiar 6 pares de letras.

Con todas las modificaciones finales la máquina Enigma ofrecía billones de posibilidades de creación de claves haciéndola prácticamente indescifrable si no tenías la clave en tu poder. El número de combinaciones posibles lo calcula Simon Singh en *Los códigos secretos* y afirma:

"La lista siguiente muestra cada variable de la máquina y el número correspondiente de posibilidades para cada una:

Orientaciones de los modificadores. Cada uno de los tres modificadores se puede situar en 26 orientaciones diferentes. Por tanto, hay 26 x 26 x 26 disposiciones: 17.576

Disposiciones de los modificadores. Los tres modificadores (1, 2 y 3) se pueden colocar en cualquier de las disposiciones siguientes: 12-3, 1-3-2, 2-1-3, 2-3-1, 3-1-2, 3-2-1: 6

Clavijero. El número de maneras de conectar, y con ello intercambiar, seis pares de letras entre 26 es enorme: 100.391.791.500

Total. El número total de claves es el múltiplo de estos tres números: 17.576 x 6 x 100.391.791.500 = ***10.000.000.000.000.000****"*[19]

Los alemanes utilizaban una nueva clave cada día, de forma que sus enemigos sólo tuvieran 24 horas para descifrarla. Como era humanamente imposible, esto convirtió a Enigma en el método más seguro hasta el momento.

[19] Singh, S, (2000), *The code book: Science of Secrecy* (p. 152). Ed. Debate

Capítulo III: La criptografía en la Biblia

La criptografía también se manifestó en ciertos escritos de la Biblia. Algunos nombres referentes a personas non gratas para las comunidades cristianas, experiencias casi sobrenaturales o amenazas al Judaísmo, no se podían expresar a veces claramente. El mensaje encriptado se hacía necesario para que los reyes de los imperios que tenían sometidos a los judíos y que renegaban de Yahveh, no entendieran nada y sólo fuera visible a los ojos del Pueblo de Dios y de sus profetas.

Tres mensajes encriptados en el Libro de Jeremías

Este profeta de la Biblia vivió en la segunda mitad del siglo VII a.C. Su familia era sacerdotal, cayó en desgracia y fue deportado por Salomón del reino de Israel al reino de Judá donde gobernaba Josías. Esta tierra fue prisionera de diferentes señores en una época difícil de enfrentamientos entre tres imperios rivales: egipcio, asirio y babilónico. Su secretario, el profeta Baruc, escribió sus oráculos, miedos y conflictos. Jeremías llora y se lamenta por sus avisos de destrucción del reino y del templo de Jerusalén a manos de los babilonios. Él, estaba también vigilado por el poder político y la casta sacerdotal.[20]

Descubrió su vocación como profeta en el año 627 y predijo la caída de los imperios ya mencionados. Este canto fúnebre (Elegía) por la ruina de las ciudades empezó por Nínive (capital del imperio asirio) en el 612 a.C.; una metrópoli de 7km cuadrados y muralla de 15 puertas, que hacía falta *tres días para recorrerla* según dejó escrito otro profeta.[21] Luego le llegó el turno a Jerusalén que la tomó el ejército babilónico. Arrasó su templo y así se produjo el exilio judío del reino de Israel y del reino de Judá, en el siglo VI a.C.

En el capítulo 25 dice:

"*A todos los reyes del norte que están cerca y lejos* […] *y a todos los reyes de la superficie terrestre. Y después de todos ellos, beberá el rey de Sesac* " [22]

El reino del norte es Asiria que cayó en manos de Egipto y **Sesac** no es ningún reino o ciudad conocida. Es un nombre encriptado. Pero "aplicamos *el Método Atbash a esa palabra, se obtiene*

[20] *Biblia de Jerusalén* (1975) Ed. Desclée de Brouwer-Mensajero, pp 1175-1177 (Introducción al Libro de Jeremías por Jesús Moya) Es el texto que se ha utilizado para mencionar versículos en este capítulo del trabajo

[21] Libro de Jonás: 3,4. Vivió en el siglo VIII a.C. Los datos de Nínive (Wikipedia) Recuperado de https://es.wikipedia.org/wiki/Nínive

[22] Libro de Jeremías: 25, 26.

Babel en hebreo, o sea la ciudad de Babilonia".[23] Este Método *atbash* se llama también del Espejo porque invierte las letras del idioma hebreo como si se tratase de un espejo. La mecánica del método ya la hemos explicado en el Capítulo 2 y consiste en que la primera letra se sustituye por la última del alfabeto, la segunda con la penúltima y así sucesivamente.

¿Por qué lo hace así Jeremías? El rey Nabucodonosor II (630-562 a.C) era el dueño de un imperio que incluía territorios vasallos como el reino de Judá. Jeremías tenía miedo de que descubriera en su profecía de destrucción y ruina, la futura caída de su reinado y de la ciudad, por eso, esconde el nombre, porque vivía en ese reino vasallo. Este aviso sobre Babilonia se repite en otro capítulo:

"¡Cómo fue tomada Sesac y ocupada la prez de toda la tierra! [...] *convertida en el espanto de las naciones"* [24]

Por último, la tercera vez que Jeremías encripta un nombre es en el capítulo 51, versículo 1. Aparece otra palabra, junto a Babilonia, **Leb Camay**, que al aplicarle Atbash da como resultado "kasdim" (caldeos) el nombre que se le daba a los habitantes de la ciudad:

"Mirad que yo despierto contra Babilonia y los habitantes de Leb Camay, un viento destructor"

Estos tres ejemplos indican que el método criptográfico Atbash era utilizado por los escritores de textos religiosos en los siglos VII y VI a.C.[25] Jeremías debía conocerlo por su familia de casta sacerdotal ya que los sacerdotes recibirían una formación más erudita.

El número de la Bestia en El Apocalipsis

Uno de los mayores ejemplos del uso de la criptografía en la religión es el famoso número 666. Se dice que es la figura oculta del emperador Nerón (37-68 d. C.) Cuando Claudio, padre adoptivo de Nerón murió en el año 54 éste se convirtió en emperador a los 16 años. Entonces las decisiones del Imperio las llevaron sus tutores pero pronto la personalidad de Nerón empezaría a acarrear problemas al Imperio.

Junto con su mujer Popea, planeó el asesinato de Agripina, su madre, pues resultaba una molestia. Nerón la condenó a muerte en el año 59. Se casó con Popea y se dedicó exclusivamente

[23] Entonces Babel se codifica como Sesac. *Un código criptográfico en la Biblia*. Recuperado de http://inside-the-trash-can.blogspot.com/2016/03/un-codigo-criptografico-en-la-biblia.html

[24] Libro de Jeremías: 51, 41 (Biblia de Jerusalén)

[25] Dávila Muro, J. (2008*) Criptografía y Seguridad: La ocultación en los textos sagrados*, UPM, CUADERNO 4 pdf, p.12

Ver también "Un código criptográfico en la Biblia". Recuperado en http://inside-the-trash-can.blogspot.com/2016/03/un-codigo-criptografico-en-la-biblia.html.

a las bellas artes mientras su mente enfermaba haciéndolo paranoico hasta puntos extremos. Obligó a suicidarse a generales pues este pensaba que estaban conspirando contra su persona. Mató a patadas a Popea cuando estaba embarazada por quejarse de haber vuelto tarde de las carreras y mandó castrar a uno de sus amantes, Esporo, con quien se casó y le obligó a vestirse como una mujer.[26]

En el año 64 ocurrió el gran incendio de Roma y Nerón fue el señalado como culpable. El escritor Tácito dijo que cuatro de los catorce distritos de Roma fueron arrasados, y otros siete quedaron dañados. La ciudad ardió cinco días y para quitarse de encima la acusación culpó a los cristianos y se convirtió en un incansable perseguidor de las primeras comunidades de San Pedro y San Pablo. A muchos los mandó crucificar (entre ellos al apóstol Pedro); fueron devorados por leones en la arena; otros vestidos con pieles de animales los echaron a los perros de caza o murieron sirviendo de antorchas humanas en los jardines de su palacio.

Figura 25[27]. *Las antorchas de Nerón* del pintor Henrik Siemiradzki (1876) Museo Nacional de Cracovia

San Juan escribe el Apocalipsis hablando de las amenazas a las siete comunidades o iglesias repartidas por el Imperio romano. Cuando habla del poder de la Bestia dice:

"¡Aquí está la sabiduría! Que el inteligente calcule la cifra de la Bestia; pues es la cifra de un hombre. Su cifra es 666" [28]

[26] Suetonio, *Vida de los doce Césares*, Ed. Juventud, Barcelona, 1978, XXIX, p. 255
[27] Imagen tomada de https://fr.wikipedia.org/wiki/Premiers_martyrs_de_l%27%C3%89glise_de_Rome#/media/File:Siemiradski_Fackeln.jpg
[28] Apocalipsis 13, 189

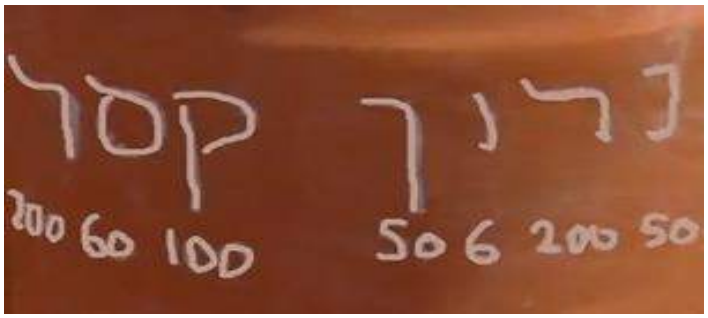


Figura 26 [29]

En la figura podemos ver escrito en hebreo "Nerón César" y los valores de cada letra debajo. Sumamos los valores: 200 + 60 + 100 + 50 + 6 + 200 + 50 = 666 es el resultado

En las últimas revisiones del tema se ha investigado que *"la cifra **666** es en numeración romana, **DCLXVI**. Este acrónimo vendría a significar:*

***D**omitius (o **D**omitianus) **C**aesar **L**egatos **X**ti **V**iolenter **I**nterfecit, que traducido es: Domicio (o Domiciano) César mató vilmente a los enviados de Cristo. Domicio es el nombre del emperador Nerón antes de ser adoptado por el emperador Claudio como hijo suyo"*[30].

Fue el 666 una cifra referente a Nerón hasta que el Cristianismo fue religión oficial.

Los mensajes crípticos durante el periodo del Cristianismo no oficial

En los años de clandestinidad de las primeras comunidades cristianas, las catacumbas también fueron una fuente de pictogramas[31] con mensajes evidentes. Pero en nuestra opinión, también aparecen algunos signos criptográficos porque los mensajes de fe quedaban ocultos al paganismo de Roma; por ejemplo, el pez y el ancla (la cruz) simbolizaban a Cristo así como el crismón.

"*Éste consiste en una X atravesada en el centro por la I, formando un anagrama que son las iniciales griegas de Iesus Xristos; más tarde, la I será sustituida por la P griega, el anagrama hace así referencia a las dos primeras letras de Xristos. Además, el conjunto suele quedar envuelto en un círculo, símbolo solar que nos habla de Cristo como sol invictus*." [32]

[29] Imagen tomada de https://www.bbc.com/mundo/noticias-36468419
[30] Recuperado de https://es.wikipedia.org/wiki/Marca_de_la_Bestia
[31] Un pictograma es un signo claro y esquemático que representa un objeto real, figura o concepto. Sintetiza un mensaje que puede informar, superando la barrera de las lenguas. El criptograma esconde el mensaje para aquellos que no están iniciados
[32] Arte Paleocristiano. Apuntes: Crismón. Universidad de La Coruña. Figuras 23-24. Recuperado de https://www.udc.es/dep/com/castellano/arte_virtual/fichas/paleocristiano/pintura/artecristiano_ficha02_l07.html

Figura 27

Figura 28[33]

Figura 29

En el siglo II la Iglesia tomó la palabra "Ichthys" (pez en griego) como símbolo de Cristo. En esta simbología, las letras de la palabra "Ichthys" representan de forma acróstica y también encriptado, las iniciales de la siguiente frase: **Iesous Christos Theou Yios Soter .**

Ichthys es igual a **I X θ Y C** en griego. Aquí presentamos su esquema

Griego	Alfabeto griego	Pronunciación en griego	Español
I	I	Iesus	Jesús
Ch	X	Christos	Cristo
Th	θ	Theou	De Dios
Y	Y	Uios	Hijo
S	Σ/C	Soter	Salvador

Figura 30

El significado es entonces: **"Jesús, Cristo, Hijo de Dios, Salvador".** [34] El símbolo del pez, el crismón y el críptico "Ichthus" fueron utilizados entre los cristianos de la Iglesia Primitiva para representar a Jesús y la nueva fe. Sólo los ojos de un creyente podía descifrarlos y esta sabiduría quedaba oculta a los paganos. El pez que se representó muchas veces en las catacumbas del siglo II, ya desapareció en el IV.

[33] Figura 23 (Foto de Juan Antonio Olañeta). Figura 24-25 (Wikipedia. Catacumbas de San Calixto)
[34] Larrauri, J. (2018) Por qué los primeros cristianos utilizaban el pez. Recuperado de: http://www.primeroscristianos.com/por-que-los-primeros-cristianos-utilizaban-el-pez-como-un-simbolo/

Capítulo IV: La criptografía en la Política y en la Diplomacia Moderna

Desde Grecia hasta el final de la Edad Media

Si miramos hacia la **Antigua Grecia**, en *La Ilíada* de Homero hay una referencia al uso del cifrado de mensajes. Belerofonte, héroe mitológico, entrega al rey de Licia una tablilla cifrada por el rey Preto de Tirinto; el contenido es secreto y el mensaje esconde que se debe dar muerte al portador de la misma, Belerofonte.

"*La divina Antea, mujer de Preto, había deseado con locura juntarse clandestinamente con Belerofonte; pero no pudo persuadir al prudente héroe, que sólo pensaba en cosas honestas, y mintiendo dijo al rey Preto: «¡Preto! Ojalá te mueras, o mata a Belerofonte, que ha querido juntarse conmigo, sin que yo lo deseara.» Así dijo. El rey se encendió en ira al oírla* […] *y le envió a la Licia; y, haciendo mortíferas señales en una tablita que se doblaba, entregole los perniciosos signos con orden de que los mostrase a su suegro para que éste lo perdiera*."[35]

Más que un mensaje de esteganografía, pudo ser de criptografía, porque el vasallo portador desconocía su futura muerte.

Se sabe que los romanos conocían la criptografía. El ejemplo más famoso es el **Cifrado de César** atribuido a Julio César (100-44 a.C.). Este cifrado que ya explicamos en el Capítulo II se basa en el desplazamiento de letras. Cada letra del texto original se tiene que sustituir por otra que está un número fijo de posiciones más adelante en el alfabeto. Según el historiador romano Suetonio, Julio César usaba un desplazamiento de 3 letras:

"*Si tenía que hacer alguna comunicación secreta lo hacía en clave , esto es, dispuesto de forma el orden de las letras que no pudiera reconstruirse ninguna palabra; y si alguno quiere investigar y descifrarlas debe sustituir cada letra por la tercera que le sigue en el alfabeto. Esto es la D por la A y así las demás." (LVI)* [36]

Octavio Augusto, el primer emperador que era sobrino-nieto de Julio César, usó solamente el desplazamiento de una letra.[37]

---

[35] Homero, La Iliada, Canto VI. Dato investigado por Velasco, Juan Jesús "Breve historia de la criptografía", *Diario Turing* (20-5-2014). Recuperado de: https://www.eldiario.es/turing/criptografia/Breve-historia-criptografia_0_261773822.html

[36] Suetonio, (1975) *Vida de los doce Césares*, Ed. Juventud, Barcelona, p. 48

[37] *"Cuantas veces escribía en clave, ponía la lera B por la A, la C por la B y así en este mismo orden con las letras siguientes, en vez de la X ponía dos A" (LXXXVIII) Ibídem* p. 113.

El método de César tenía algunas ventajas. No hacía falta un libro de signos fantásticos. Solo necesitabas conocer el alfabeto latino de 23 letras y saber entonces que solo podía haber 22 posiciones posibles como ha estudiado Kroll[38].

Durante la Edad Media, la criptografía siguió evolucionando gracias al mundo árabe que daría a conocer el **criptoanálisis**: descifrar un mensaje oculto sin conocer la clave o el método que se ha usado para encriptarlo. Este método estadístico se descubre en el siglo IX en Bagdad, en la *Casa de la Sabiduría* donde está el filósofo, matemático y criptólogo **Abu Yusuf Al-Kindi .** Él escribirá un documento (*Manuscrito para descifrar mensajes criptográficos*) que recoge el uso de métodos estadísticos y sienta las bases para romper mensajes cifrados en el futuro. [39]

La España Moderna

Soler Fuensanta se ha dedicado a estudiar este periodo y recoge que en los preparativos para la Conquista de Granada, los Reyes Católicos tuvieron correspondencia secreta y utilizaron una cifra o diccionario de 2400 términos, sílabas, palabras o letras.[40] Colón y Hernán Cortés también utilizaron caracteres cifrados para los avisos y correos oficiales con el Nuevo Mundo.[41]

Pero de esta época, la noticia más destacada es la correspondencia secreta y cifrada entre el Gran Capitán Gonzalo Fernández de Córdoba y Fernando el Católico durante la campaña de Nápoles contra Francia. El código en clave ha estado oculto durante más de 500 años en tres cartas (Archivo de los duques de Maqueda) y ha sido descifrado en 2018.[42] Son de 1502-1506 y dan instrucciones, llamadas al orden del rey al Gran Capitán, amenazas veladas, envío de más tropas, más recaudación de impuestos. También hablan sobre la conveniencia de impulsar el matrimonio entre las viudas del lugar y los soldados españoles para que hubiera más integración

[38] Kroll, S. (2016) . "Evolución de los sistemas criptográficos desde la Edad Media a la Moderna" Revista *Memoria y Civilización* 19 Universidad de Navarra, pp.184 Recuperado de: https://www.unav.edu/publicaciones/revistas/index.php/myc/article/view/7665/7302 pp. 181-199

[39] Kroll, p. 186. Este análisis de frecuencia (técnica que se usaría durante la II G.M) se basaba en analizar patrones en los mensajes cifrados para localizar repeticiones y buscar la correlación, con la probabilidad de que aparezcan ciertas letras en un texto escrito en un idioma concreto .

[40] Soler Fuensanta, J.R. *La criptologia española hasta el final de la Guerra Civil*, p.3. Recuperado de: http://www.criptohistoria.es/files/historia.pdf

[41] Ibídem, pp. 4-5. Los códigos para la flota de Indias eran de baja calidad porque los mandos tenían orden de echar al mar la correspondencia delicada si había peligro de asalto al barco.

[42]Tena, Berta.(2-2-2018) "*El CNI descifra las cartas secretas entre Fernando el Católico y el Gran Capitán de la campaña de Nápoles"* EL PAIS . Recuperado de: https://elpais.com/cultura/2018/02/02/actualidad/1517583621_006550.html y también en: http://www.museo.ejercito.es/noticias/noticias/CARTA_DESCIFRADA_FERNANDO_EL_CATOLICO_AL_GRAN_CAPITAN.html

social y "*así ganarse a los nuevos súbditos*". El Gran Capitán también hace preguntas privadas para saber cómo están los familiares de personas conocidas de la Corte.

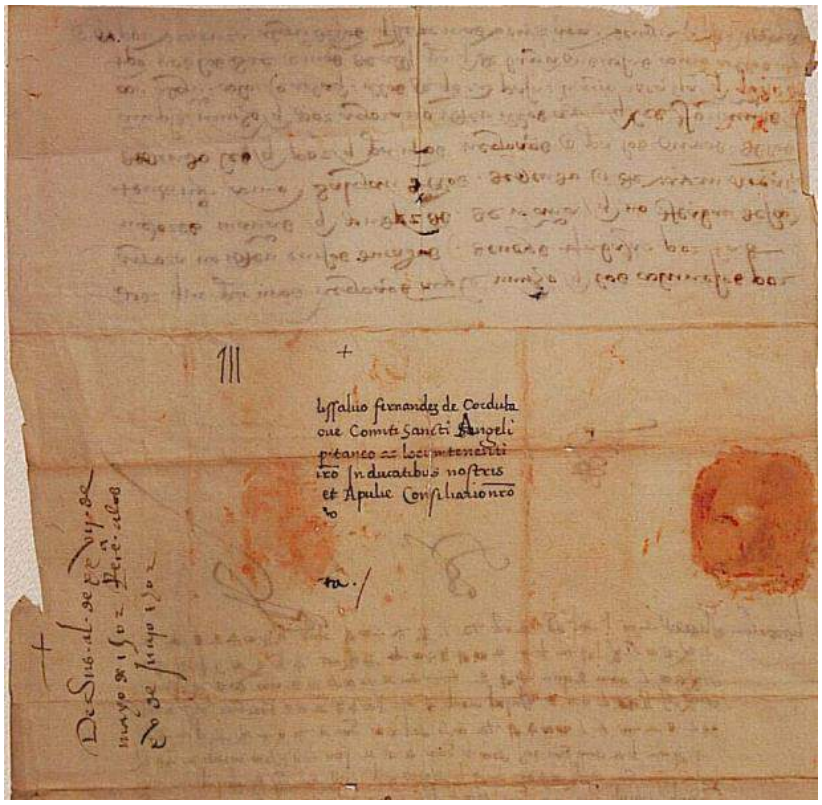


Figura 31. Portada de la carta de Fernando el Católico dirigida a Gonzalo Fernández de Córdoba, duque de Santángelo. Escrita el 27 de mayo de 1502

Cuando se expusieron en 2015 en el Museo del Ejército, se descubrió que en una misma hoja había un fragmento de carta con notas del Gran Capitán, sobre su traducción. Era como un trozo de la piedra de Rosetta[43] y los expertos del CNI encontraron así la clave para analizarlas. Tablas del rey Católico estaban muy bien pensadas porque su código es un precursor del sistema Vigenère, pero bastante avanzado: 88 símbolos y 237 códigos de letras (Véase Anexo II).

13	14	13	15	16	17	18	13	17	00	19	20	21	13	22	moc	10	13	22
e	?	e	?	i	s	t	e	s		s	a	?	e	?	con	v	e	?

mv	12	27	10	16	28	27	00	ran	rnp	neb	sa	32	neb	snc	00	48	27	39
?	m	o	v	i	d	o		por	?	?	?	?	?	?		d	o	n

[43]La piedra de Rosetta fue hallada en 1799 por el ejército francés de Napoleón. Tenía tres inscripciones en egipcio, demótico y griego antiguo. Los estudiosos comprobaron que era un mismo texto en tres lenguas. Champollion, siguiendo el texto griego pudo descifrar los jeroglíficos egipcios en 1822. Actualmente está en el Museo Británico. Recuperado en:
https://www.nationalgeographic.com.es/historia/actualidad/la-piedra-de-rosetta-se-descubrio-hace-214-anos_7462/1

Figura 32[44]. Combinatoria realizada por el CNI sobre las cartas. Las palabras cifradas no tienen separaciones para no detectar los finales y principios. Hay símbolos sueltos, que corresponden a letras pero no siempre son los mismos. Las de más uso tienen 5 ó 6 caracteres figurativos como triángulos rayas o números, con lo que no se pueden detectar las repeticiones.

Bajo el reinado de Felipe II, el rey comunicaría a todos sus reinos que cambiaría e innovaría la cifra de su padre. En aquella época las conspiraciones, traiciones y sabotajes eran una constante que creó un ambiente de desconfianza entre los reinos europeos. Felipe era consciente y quiso reforzar la fallida clave de Carlos I que en múltiples ocasiones habían desencriptado tanto franceses como italianos.

El Rey Prudente usó varios **nomenclátor**, la **cifra general** destinada a la comunicación entre el rey y los ministros; las cifras extranjeras y particulares para comunicaciones entre el duque de Alba, gobernadores y embajadores en varios países y otros nomenclátor para sus comunicaciones con América. Estas cifras las cambiaba cada tres o cuatro años y, cada cambio era comunicado por el Despacho Universal.

[44] García Calero (2-2-2018) "El CNI descifra uno de los grandes misterios de la Historia de España, el ´código del gran Capitán" ABC Cultura Recuperado de: https://www.abc.es/cultura/abci-descifra-grandes-misterios-historia-espana-codigo-gran-capitan-201802020247_noticia.html
Todas la imágenes del cifrado en
http://www.museo.ejercito.es/Galerias/documentos/Sistema_de_cifra_y_codigos.pdf
http://www.museo.ejercito.es/Galerias/documentos/Carta_del_Rey_Fernando_el_Catolico_al_Gran_Capitan.pdf

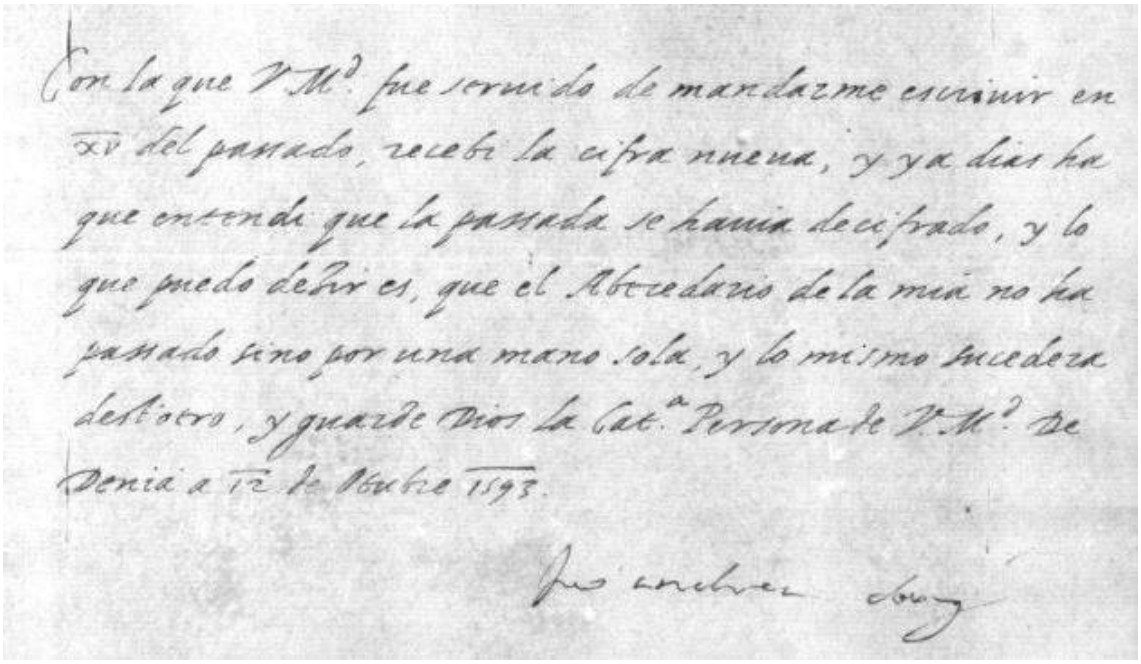

Con la que V.Md. fue servido de mandarme escrivir en
XV del passado, recebi la cifra nueva, y ya dias ha
que entendi que la passada se havia decifrado, y lo
que puedo dezir es, que el Abecedario de la mia no ha
passado sino por una mano sola, y lo mismo sucedera
del otro, y guarde Dios la Catª Persona de V.Md. De
Denia a 12 de Otubre 1593.

Figura 33[45]. Con la que V.M[d]. fue servido de mandarme escrivir en XV del passado, recibi la cifra nueva, y ya dias que entendí que la passada se havia decifrado, y lo que puedo decir es, que el Abecedario de la mia no ha pasado sino por una mano sola, y lo mismo sucedera del otro, y guarde Dios La Catª Persona de V.M[d]. De Denia a 12 de Otubre 1593. juan andrea doria

Estos cifrados mostraban una complejidad muy superior a los nomenclátor de Carlos I. Elevaron el número de sustituciones, incluyen homófonos, caracteres nulos, bigramas, trigramas y un código con las palabras más comunes. Todo esto sumado a la existencia de los cifrados particulares hicieron de la criptografía de Felipe II una de las mejores de la época. A pesar de ello fue criptoanalizada con éxito por François Viète (1540-1603), un conocido matemático y criptoanalista al servicio del rey Enrique IV. Felipe II, al no poder detenerle, acusó a Vietè de brujería ante el Papa. Esta denuncia fue archivada pues el mismo equipo criptográfico del Papa había logrado con anterioridad el criptoanálisis de los códigos españoles.

La Europa Moderna

Los sistemas criptológicos tienen éxito a partir de los siglos XIV-XV por tres motivos importantes que explica Kroll (2016) Se extiende el uso del papel en lugar del pergamino, aparece el servicio postal monopolizado por el Estado que tiene una red de empleados de correos y caballos, y aparece la Diplomacia (embajadores y embajadas). Los primeros estados europeos que tuvieron

[45] *Carta de Juan Andrea Doria, príncipe de Melfi, a Felipe II, rey de España, acusando el recibo de la nueva cifra*. Portal de Archivos Españoles. Recuperado de http://pares.mcu.es/ParesBusquedas20/catalogo/show/3626513

embajadores fueron Venecia, Milán y Florencia. "*La Diplomacia necesitaba de secretos"* y el embajador como tenía que comunicar cosas a su Corte, era considerado *"un espía honrado"*[46] .

Nicolás de Maquiavelo en el siglo XVI critica en sus tratados de Política que las instituciones militares no tengan cifras y sigan con métodos antiguos. Escribió sus propias ideas de secretos militares en *El arte de la guerra* (1520) para que lo conocieran los Médici de Florencia.

"*Los sitiados se valen de diferentes medios para enviar avisos a sus partidarios. No mandándolos verbalmente, los escriben en cifra y los esconden de diferentes modos. Las cifras están convenidas entre los que se corresponden con ellas y la manera de ocultarlas varía según hemos dicho. Unos han guardado las cartas en la vaina de la espada […] en el collar de los perros; otros han escrito en una carta cosas insignificantes, y después, entre líneas, con un líquido especial que, mojado o calentado el papel, aparecen letras.. "* [47]

Los reyes y los papas buscaron desde el siglo XV a los mejores matemáticos y especialistas en criptografía. Una de las figuras clave fue Leon Battista Alberti, secretario personal de tres Papas. Alberti, desarrollaría un sistema de codificación mecánico (basado en dos discos) conocido como el **Cifrado de Alberti**. Fue la gran innovación que abrió una nueva época: el primer sistema de cifrado polialfabético. La criptografía se hizo más famosa.[48]

Pero el gran reto de los descifradores de códigos del Renacimiento, fue y es todavía el **Manuscrito Voynich.** Es un texto ilustrado de más de 500 años cuyo contenido es ininteligible porque su código no se ha podido romper. Además presenta imágenes de plantas desconocidas y escenas con significado extraño. La primera noticia del manuscrito es de 1580. El emperador Rodolfo II de Habsburgo, muy interesado en las ciencias ocultas, la magia y las rarezas de todo tipo, lo compró por 600 ducados a los ingleses John Dee, un mago, y Edward Kelley, un estafador.

En el siglo XVII el manuscrito pasó por varios dueños hasta que llegó a Roma y lo compró en 1912 el experto en libros antiguos y antigüedades Wilfrid Voynich, de ahí su nombre. En 1931, su viuda lo vendió a un anticuario neoyorquino, Hans Peter Kraus, que no consiguió revenderlo y lo regaló a la Universidad de Yale en 1969.[49]

---

[46] Kroll, p.190

[47] Maquiavelo (1520) *El arte de la guerra,* p. 119. Es un tratado militar de la Edad Moderna para los Médici. Recuperado en: https://freeditorial.com/es/books/del-arte-de-la-guerra/related-books

[48] "Una creciente demanda a nivel europeo generó esta multiplicación de ideas innovadoras después de cientos de años de estancamiento" (Kroll , p. 194)

[49] Corral, J. L.(2018) "El códice Voynich, el manuscrito más extraño del mundo" *National Geographic España* (1-02-2018) Recuperado en: https://www.nationalgeographic.com.es/historia/grandes-reportajes/codice-voynich-manuscrito-mas-extrano-del-mundo_12344/1

Figura 34

Escrito sobre pergamino fino, tiene 232 páginas, centenares de dibujos y 37.919 palabras con 25 caracteres distintos. No tiene autor, título, ni fecha ni capítulos. En la foto inferior aparece Wilfrid Voynich quien lo compró.

Figura 35 [50]

Muchos han tratado de descifrarlo. Lo intentó un profesor de la universidad de Pensilvania en 1921 y se trastornó porque es casi un jeroglífico. Visualmente parece escrito por una sola mano, con letras homogéneas y muy regulares, prácticamente idénticas, sin un solo error, algo muy curioso en un manuscrito. Además está escrito de izquierda a derecha, sin signos de puntuación ¿Se utilizaría alguna plantilla? Quizá el enigma se quede sin resolver.

A comienzos de este año 2018, la prensa dijo que informáticos de la Universidad americana de Alberta (Canadá) han logrado descubrir que se trata de un volumen escrito empleando alfagramas hebreos antiguos. Lo consiguieron sometiendo el manuscrito a una inteligencia

[50] Ibídem. Huído de Rusia por motivos políticos, el polaco Wilfrid Voynich se fue a Inglaterra donde trabajó como tratante de libros raros. Estaba convencido de que el tratado ocultaba conocimientos de alquimia

artificial creada para entender las ambigüedades humanas en el lenguaje y descubrir la lengua en la que está escrito. Ahora hay que buscar historiadores especializados en hebreo antiguo, pero la parte más difícil ya se conoce [51]

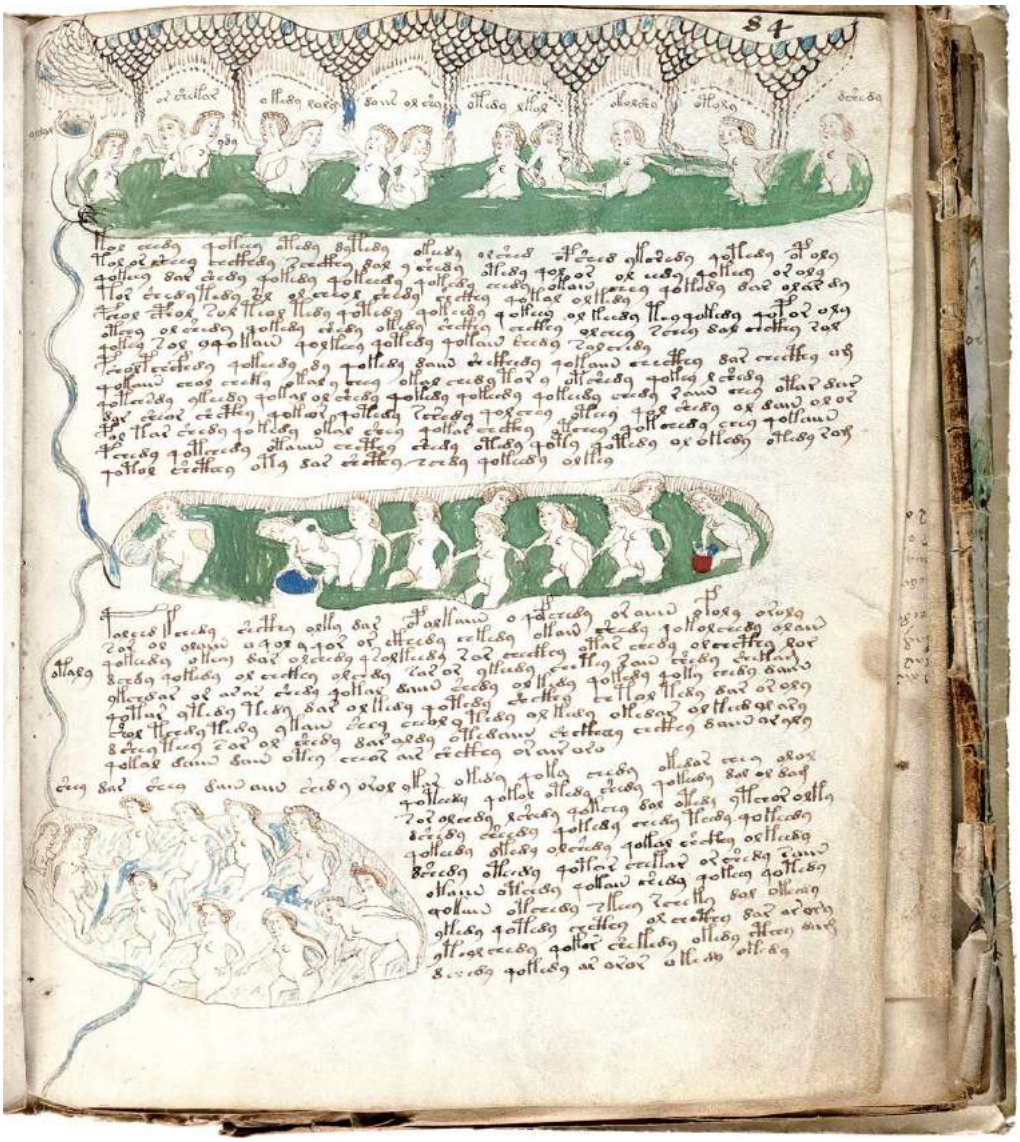


Figura 36

En Francia aparece Antoine Rossignol (1600-1680) un matemático que se convertiría desde 1628, en uno de los criptógrafos más importantes y tanto su hijo como su nieto, trabajarían en el primer centro de criptología francés conocido como "Cabinet Noir du Roi" elaborando *La Gran Cifra*, un Nomenclátor que fue muy bueno en su clase y utilizado por Luis XIV en sus correspondencias militares.[52] Este Despacho privado o Servicio Secreto se convertiría en "*The*

[51] Ollero, Daniel (2018) "Una inteligencia artificial descifra el códice Voynich, el libro más misterioso del mundo" EL MUNDO (30/01/2018) Recuperado en: https://www.elmundo.es/tecnologia/2018/01/30/5a6f515846163f48798b459f.html

[52] Dávila Muro, p. 32.

Black Chamber" un término internacional para otros países. Durante el siglo XVIII la criptografía estuvo presente en la mayoría de conflictos bélicos. Tendría un papel clave en la "Guerra de la Independencia" de las colonias británicas en América al interceptar los mensajes del Ejército Británico y también al aparecer nuevos métodos de cifrado como la famosa Rueda de Madera de Thomas Jefferson (1790).

Figura 37

Capítulo V: La criptografía en las hazañas bélicas

La Guerra Civil Española

En el verano de 1936, el general Francisco Franco (1892-1975) lleva a cabo un alzamiento militar, da un golpe de estado que fractura España e iniciará la Guerra Civil española. El bando nacional y el bando republicano pretenden controlar el país, desde los territorios que cada uno domina. A los republicanos los apoyan intelectuales de izquierdas, sindicatos, obreros de zonas industriales, comunistas, así como la población de las ciudades importantes. El bando franquista tenía el soporte de las altas clases, de la Iglesia, y de los partidos de extrema derecha europeos que veían a las izquierdas y al comunismo como una amenaza para los negocios de los países de Europa Occidental.

Todas las guerras requieren de una gran comunicación entre los integrantes de los distintos bandos, información de la organización del siguiente asalto, datos confidenciales del propio bando, cambios en las cadenas de mando… avisos que en ningún momento debía conocer el enemigo. Por ello ambas partes echaron mano de la criptografía pero su utilización se había estancado hacía tiempo[53] y sus avances eran prácticamente nulos.

La Guerra Civil consistió en una batalla hermanos contra hermanos lo que significaba que todos habían estudiado en los mismos lugares, con los mismos medios y por tanto, los métodos criptográficos que conocían eran los mismos. Una situación sin duda curiosa y, como afirmó el almirante Cervera: *"Nada se nos resistía, ya que eran simples claves de transposición y en esta materia estábamos, tanto los nacionales como los rojos, en mantillas"*[54].

Era evidente que ante la falta de formación de ambos bandos, el descifrado de los mensajes fuera algo previsible cuando no habitual.

Los métodos más utilizados fueron las tablas de sustitución generalmente numéricas y con homófonos y nulos extraídos de nomenclatores poco conocidos. A este método se le llamó el **cifrado de cinta**, pues, a partir de una cinta con el abecedario y los correspondientes valores numéricos (homófonos) de cada letra, se escribían los textos. Al emplear homófonos lograrían eludir el criptoanálisis por frecuencia pero no dejaría de ser un sistema simple y fácil de descifrar. Por ello se creó el cifrado de cinta móvil, que añadía una cinta desplazable que variaba los homófonos, de forma que hacía más complejo su criptoanálisis.

[53] El general del ejército carlista, Zumalacárregui, utilizó el zumo de limón.

[54] Soler Fuensanta, J. R. *La Criptología Española hasta el final de la Guerra Civil*. Recuperado de https://docplayer.es/13097526-La-criptologia-espanola-hasta-el-final-de-la-guerra-civil-jose-ramon-soler-fuensanta.html

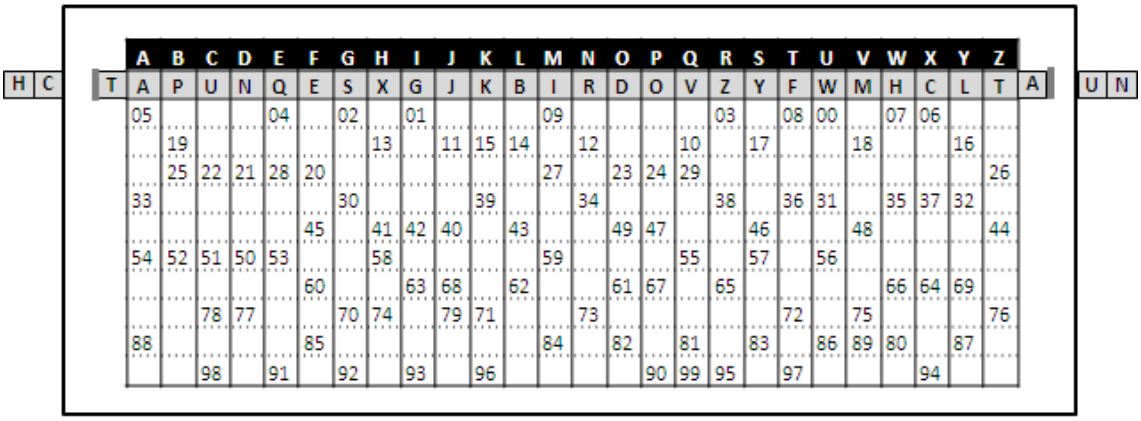


Figura 38[55]. La cinta móvil es la que se encuentra en la segunda fila. Emisor y receptor acordaban una posición y a partir de ahí las letras cambiaban de homófonos según se desplazara la cinta móvil. El mensaje se encriptaría cogiendo cada letra, y escogiendo cualquier homófono de los que le corresponden según la segunda cinta.

El bando nacionalista tuvo a su servicio a grandes criptoanalistas que trabajaban en el Estado Mayor de Zaragoza y de Palma de Mallorca, que enviaban sus desencriptados al Cuartel General de Franco, lugar donde se centralizaban todas las claves descubiertas. Adquirieron diez máquinas Enigma para la guerra así como máquinas Kryra, pero no se vieron capaces de utilizarlas ante la complejidad de las mismas y por ello terminaron recurriendo a los métodos clásicos: el libro de códigos con una lista de homófonos y los sistemas de cinta.

En cuanto al bando republicano el desencriptado recayó sobre el gabinete de contracifra del Servicio de Información del Estado Mayor. Fueron además apoyados por Rusia, quien les asesoró en el ámbito criptográfico y entrenó a sus criptoanalistas. Prefirieron basar su seguridad en un amplio abanico de métodos que fueron los sistemas de cinta, los libros de códigos y los códigos de trinchera. Su efectividad fue deficiente como afirma Soler Fuensanta mientras que el bando nacional, con su centralización, logró por ejemplo la captura del buque Mar Cantábrico que traía armas para el ejército de la República en marzo de 1937.

La Segunda Guerra Mundial

La criptografía fue clave durante la Segunda Guerra Mundial y de hecho, hizo cambiar el curso de la guerra. Alemania había conseguido dominar el Atlántico Norte con su flota de submarinos. Sus comunicaciones eran indescifrables para los Aliados gracias a la máquina Enigma. Además de los frentes bélicos por tierra, mar y aire, se abría un nuevo campo de batalla: romper las comunicaciones enemigas. Esta tarea la encargaron los Aliados a un grupo de matemáticos,

[55] García Lagarran, M. (2016). *Criptografía (XXXIII): cifrado cinta móvil (I).* [Figura] Extraída de http://mikelgarcialarragan.blogspot.com/2016/10/criptografia-xxxiii-cifrado-cinta-movil.html

ingenieros y físicos que trabajaron desde las instalaciones de Bletchley Park (Londres) y entre los que se encontraba Alan Turing.

Figura 39[56]

Ellos fueron los criptoanalistas que lograron descifrar Enigma y a pesar de ser la hazaña más conocida, no fue la única. Los métodos criptográficos durante las dos guerras mundiales fueron muy usados.

Estados Unidos

Estados Unidos reutilizó una técnica que había empleado con éxito en la Primera Guerra Mundial. En vez de usar complejos algoritmos matemáticos utilizaron como código las desconocidas lenguas de los nativos americanos.

Bajo el mando de Estados Unidos se encontraban medio millar de nativos americanos que servían como operadores de radio y cifraban en su lengua los mensajes para que el ejército japonés no lograra entender nada de lo que se transmitía. Los navajos, meskwakis y comanches fueron algunos de los pueblos indígenas que sirvieron a su patria en la II G.M. en África, Europa y el Pacífico.

El hijo de un misionero, Philip Johnston, sugirió al Comandante General Clayton B. Vogel, Jefe del Cuerpo Anfibio de la Flota del Pacífico, que utilizara la lengua de los navajos.

Johnston había vivido muchos años con la tribu y hablaba fluidamente el navajo. Creía que el idioma se podía usar como código, porque su dificultad garantizaría la seguridad de las

[56] *Un modelo raro de la máquina nazi Enigma bate un récord en subastas.* (23-10-2015). EL PAÍS.

transmisiones. Como el idioma navajo no tenía prácticamente escritura, era completamente ininteligible para un extranjero que intentara descifrarlo, y mucho menos leerlo.

Solo siete meses después de hacer la sugerencia, ya había miembros de la tribu Navajo en los cuerpos de la Marina. En un principio, solamente se reclutaron 29 que comenzaron a entrenarse en Camp Pendleton en mayo de 1942. Con el tiempo, se entrenaron en el uso del código más de 400 miembros de la tribu y menos de 30 hablantes no nativos podían entender el idioma. De los Navajo entrenados y correctamente equipados, aproximadamente 300 fueron enviados al campo de batalla, donde conocieron el peligro incluso de parte de los de su propio bando. Algunos infantes de Marina confundieron a los Navajo con japoneses y los mataron.

La existencia de los codificadores se mantuvo en secreto hasta 1968, ya que se especulaba que quizá los militares quisieran utilizarlos en otra guerra. En 1981, el presidente Ronald Reagan otorgó a los codificadores un Certificado de Agradecimiento. Veinte años más tarde, después de una campaña del senador Jeff Bingaman, en julio de 2001 el presidente George W. Bush condecoró a los 29 codificadores originales con una Medalla de Oro del Congreso. En el momento de la ceremonia, solo quedaban vivos cinco de los 29. Los supervivientes de esta tribu, recibieron unos meses después una Medalla de Plata del Congreso en Window Rock (Arizona) la capital de la Nación Navajo.[57]

Figura 40: Lloyd Olivier (en el centro) con dos camaradas navajos en 1943

En el frente del Pacífico criptoanalistas de Estados Unidos, Holanda y Gran Bretaña se unieron para romper el código naval japonés JN-25 y lograron conocer los planes bélicos de Japón en Midway.

[57] Antón, J. (2011) *Lloyd Olivier, codificador navajo de los marines*, EL PAÍS Recuperado de https://elpais.com/diario/2011/03/26/necrologicas/1301094002_850215.html

Polonia

En los años 20 Polonia no podía desistir del intento de descifrar Enigma, por ello, el Servicio de Descifrado del ejército polaco, el *Biuro Szyfrów,* intentó desesperadamente avanzar en el desencriptado. Se unieron nuevos y prometedores miembros al Biuro y consiguieron los documentos técnicos confidenciales sobre Enigma gracias a los Servicios Secretos franceses. Con ello pudieron hacer una reproducción más o menos fiel de lo que era Enigma; pero no bastaba. Lo que hacía indescifrable a Enigma era su clave escondida entre miles de billones de configuraciones.

Con el tiempo los polacos elaboraron unas tablas que contenían "cadenas" de letras cifradas que sabían que tenían relación entre sí. A partir de las cadenas determinaron el número de "enlaces" de cada una de ellas. Comparando las tablas entre sí de días iguales y distintos llegaron a la conclusión de que:

- Las tablas variaban conforme lo hacía la clave, lo que implicaba una relación entre ambas.
- El número de enlaces no se modificaba con independencia de la configuración del tablero de conexiones que intercambiaba los pares de letras.

Estos descubrimientos implicaron que no necesitaran encontrar una clave específica sino limitarse a averiguar la posición inicial de los rotores entre unas 100.000 opciones posibles. Gracias a la réplica que habían construido pudieron probar todas las alternativas en ella y definir el número de enlaces en cada clave para después compararlos con los correspondientes a cada mensaje y con ello saber la combinación inicial de los rotores. Así lograban un descifrado parcial, sólo les faltaba descubrir los pares de letras intercambiados por el tablero de conexiones.

Construyeron una máquina que haría automáticamente esta compleja y tediosa tarea a la que llamaron "bomba". Con estos artefactos lograron descifrar con cierta rapidez comunicaciones secretas, a pesar del gran avance que consiguieron, los alemanes añadieron como medida de precaución 2 rotores más y ampliaron el número de clavijas posibles de 6 a 10. Esto fue el fin de todo el esfuerzo que el Biuro había hecho.

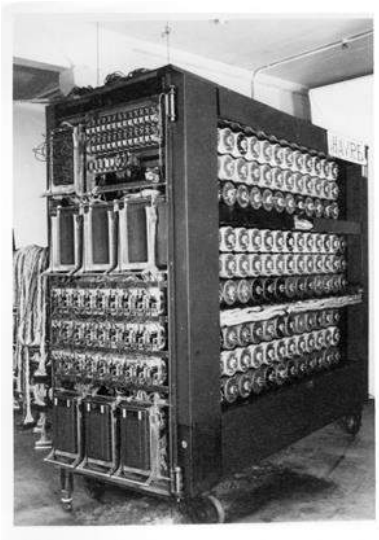
El 1 de septiembre de 1939 Alemania invade Polonia y dos días después da comienzo la Segunda Guerra Mundial.

Bletchley Park

Poco antes de ser invadida, Polonia compartió todos sus avances del descifrado de Enigma con los ingleses. Esta información llegó a la Escuela Gubernamental de Codificación y Cifrado, en Bletchley Park a 80 km de Londres.

Figura 41[58]

De entre sus criptoanalistas destacamos a Alan Turing, quien descifraría finalmente a Enigma teniendo su sitio en la Historia. Los primeros pasos de los ingleses fueron crear nuevas y más eficientes bombas y siguieron la estrategia polaca basada en la doble repetición de la clave diaria.



A la hora de escoger clave (key) solemos decantarnos por combinaciones fáciles de recordar, lo mismo sucedió a los operadores alemanes. Un ejemplo de ello fue que uno de los operadores utilizaba frecuentemente la clave CIL. Eran las iniciales de su novia. Gracias a este operador, los ingleses probaban sus bombas con esta clave y fue mucho el tiempo que les ahorró.

Turing descubrió un modo de fragmentar el irrompible cifrado de Enigma. Se dio cuenta de que los mensajes militares y diplomáticos de los alemanes mantenían una estructura fija. Por ejemplo en un mensaje naval era muy común encontrar información sobre la posición, velocidad del navío o el tiempo en alta mar.

Gracias a la inmensa cantidad de mensajes que previamente habían desencriptado tenían una idea muy precisa de la estructura de los mencionados textos y las palabras que repetían así como

[58] Miret, J.M. (2013) *Alan Turing: el descifrado de la máquina Enigma.* Recuperado de http://blogs.elpais.com/turing/2013/06/alan-turing-el-descifrado-de-la-maquina-enigma.html

la posición de algunas de ellas (“Posición”, “Velocidad”) y su correspondiente cifrado. A esas palabras las llamaron *cribs*.

Turing finalmente diseñó una nueva bomba que podía analizar de manera mecánica los diferentes *cribs* que se encontraban en los mensajes. La desarrolló junto con otro matemático llamado Gordon Welchman por lo que su bomba se llamó “Bomba Turing-Welchman” (hoy en Bletchley Park).

La máquina Lorenz

Surgieron nuevos y mejores cifrados entre las comunicaciones alemanas después de que se resolviera Enigma, cifrados que nadie era capaz de resolver. Nadie lo había resuelto, porque no se había cifrado con una máquina Enigma, sino con una máquina nueva: Lorenz.

Figura 42[59]

Era un nuevo sistema de cifrado que se basaba en la “libreta de un solo uso” y empleaba varios métodos a su vez, lo que la hacía invulnerable a cualquier tipo de ataque. Consistía en transformar los caracteres del mensaje a un sistema binario y lo combinaba con caracteres binarios pseudoaleatorios (de único uso) y obtenían así el ciphertext. Los mensajes los enviaban a través de un teletipo o cinta donde se marcaban los ceros y unos con “no perforado” o “perforado”.

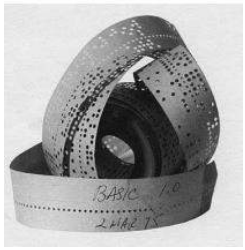


Figura 43[60]

[59] Zahumenszky, C (5-31-2016) *Encuentran un teleprinter nazi de la Segunda Guerra Mundial en Ebay y lo compra por 13 euros*. Recuperado de https://es.gizmodo.com/encuentra-un-teleprinter-nazi-de-la-segunda-guerra-mund-1779576388

[60] Gutiérrez, A. *Criptografía y criptoanálisis en las dos guerras mundiales. Ed. ACTA.*

Las Lorenz tenían un gran parecido a Enigma, por su teclado y un sistema compuesto por doce rotores. Al no ser caracteres completamente aleatorios daba un margen de vulnerabilidad pero el cifrado seguía siendo prácticamente inexpugnable. Hasta que se cometió un error colosal que terminó con la máquina Lorenz.

Uno de los operadores que transmitió dos versiones distintas de un mismo mensaje utilizó la misma clave para ambos. Fue tan simple como comparar uno y otro. Al año siguiente los ingleses construyeron una réplica y con ello descifraron completamente la máquina de Lorenz.

Conclusiones

Tras finalizar la investigación, podemos llegar a la conclusión de que la seguridad de la información se basa en tres medidas a lo largo de la historia: la *confidencialidad o* información cifrada disponible solo para personas autorizadas; la *integridad* y modificación de la información solo por personas capacitadas y la *disponibilidad* de códigos y criptosistemas para quienes lo necesitan. Y todo esto ha sido dado por la criptografía.

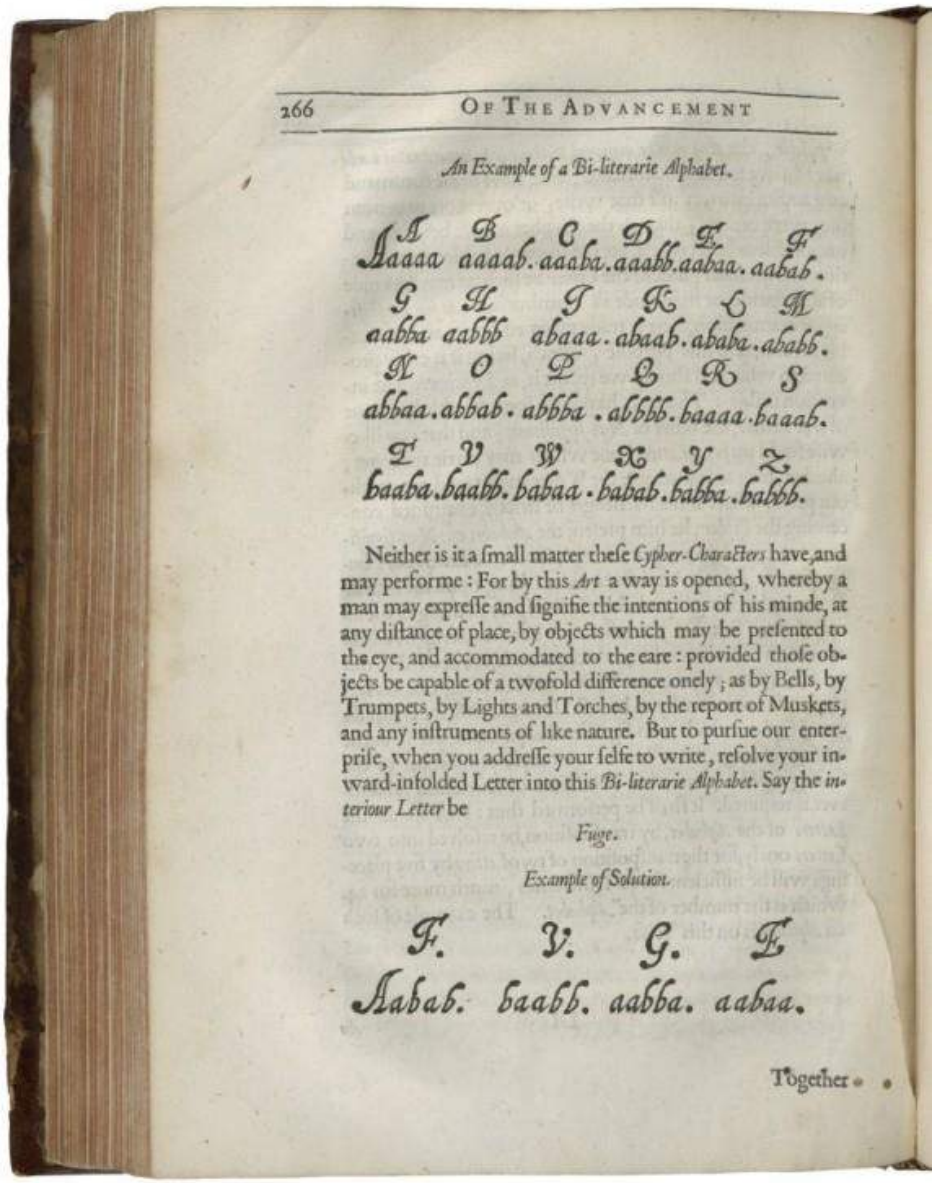
Su paso por la historia no debe de ser pasado por alto. Hemos visto que su aparición en la Biblia manifiesta el peligro que corrían profetas y primeros cristianos, motivo por el que fue una herramienta usada, y así lo plasmaron Jeremías y San Juan. Desde la Diplomacia Moderna, alcanzó una gran popularidad y grandes reyes hicieron uso de la misma para su política exterior e interior. Y en hazañas bélicas no han sido pocas las veces que la criptografía se convirtió en instrumento de vital importancia para los bandos bélicos.

Este trabajo ha significa mucho más de lo que pude inicialmente imaginar. Me ha abierto los ojos a un mundo al que nunca se me hubiera ocurrido acceder y que, gracias a las puertas que se me han abierto he logrado apreciar la inmensidad del mismo. Me siento también dichosa por haber logrado, comprender qué ha sido la criptografía para la historia. Ha supuesto un antes y un después en la forma de mirar la criptografía llevándome a querer estudiar una de las ramas de las que la criptografía fue madre: la Ciberseguridad.

Anexos

Anexo I

El avance del Saber (1605) de Francis Bacon. Donde pone de manifiesto su nueva forma de cifrado.



266 OF THE ADVANCEMENT

An Example of a Bi-literarie Alphabet.

A	B	C	D	E	F
aaaaa	aaaab.	aaaba.	aaabb.	aabaa.	aabab.
G	H	I	K	L	M
aabba	aabbb	abaaa.	abaab.	ababa.	ababb.
N	O	P	Q	R	S
abbaa.	abbab.	abbba .	abbbb.	baaaa.	baaab.
T	V	W	X	Y	Z
baaba.	baabb.	babaa.	babab.	babba.	babbb.

Neither is it a ſmall matter theſe *Cypher-Characters* have, and may performe: For by this *Art* a way is opened, whereby a man may expreſſe and ſignifie the intentions of his minde, at any diſtance of place, by objects which may be preſented to the eye, and accommodated to the eare: provided thoſe objects be capable of a twofold difference onely; as by Bells, by Trumpets, by Lights and Torches, by the report of Muskets, and any inſtruments of like nature. But to purſue our enterpriſe, when you addreſſe your ſelfe to write, reſolve your inward-infolded Letter into this *Bi-literarie Alphabet*. Say the *interiour Letter* be

Fuge.

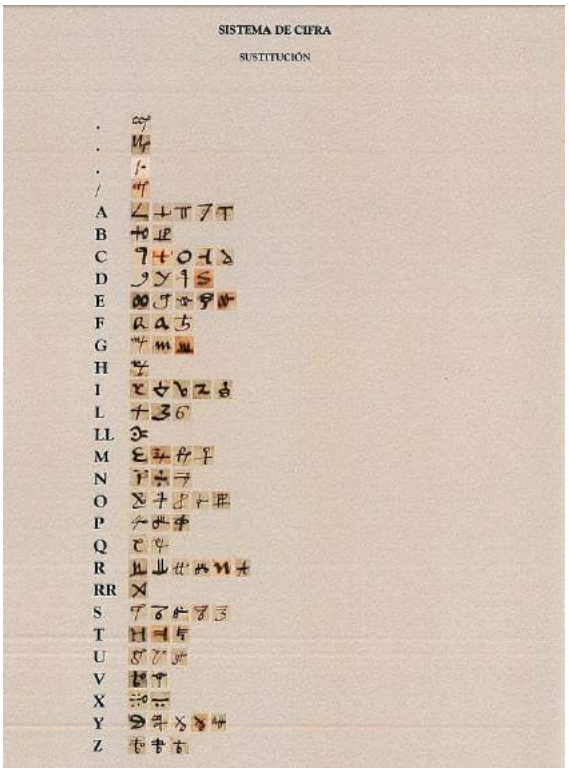
Example of Solution.

F.	V.	G.	E
aabab.	baabb.	aabba.	aabaa.

Together

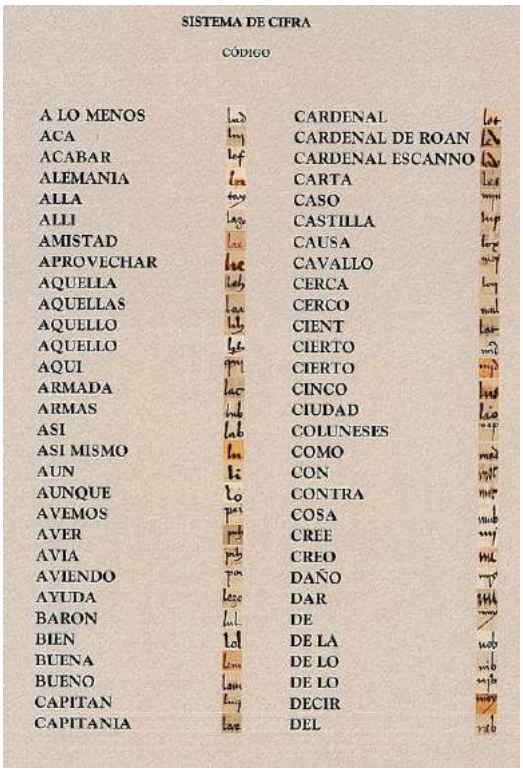
Anexo II

La cifra del Fernando el Católico y el Gran Capitán descifrado por el Centro Nacional de Inteligencia (CNI).


SISTEMA DE CIFRA

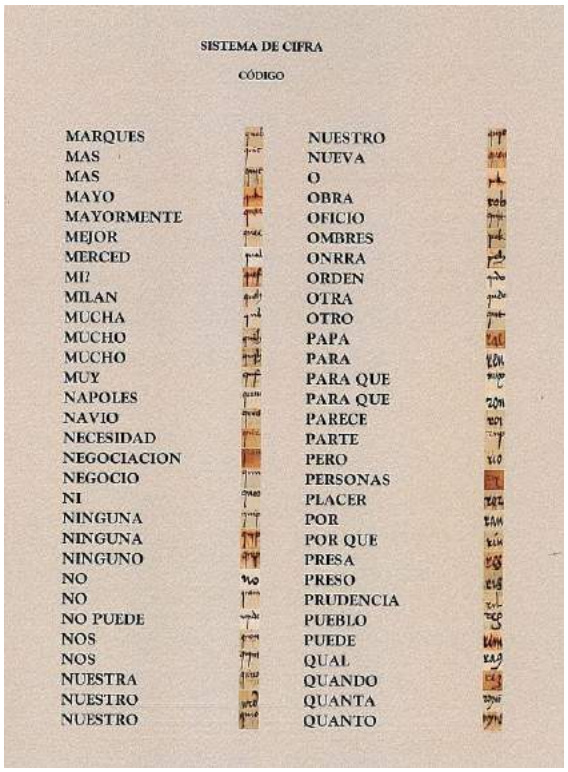
SUSTITUCIÓN

. .
. .
. .
/ /
A A
B B
C C
D D
E E
F F
G G
H H
I I
L L
LL LL
M M
N N
O O
P P
Q Q
R R
RR RR
S S
T T
U U
V V
X X
Y Y
Z Z


SISTEMA DE CIFRA

CÓDIGO

A LO MENOS		CARDENAL	
ACA		CARDENAL DE ROAN	
ACABAR		CARDENAL ESCANNO	
ALEMANIA		CARTA	
ALLA		CASO	
ALLI		CASTILLA	
AMISTAD		CAUSA	
APROVECHAR		CAVALLO	
AQUELLA		CERCA	
AQUELLAS		CERCO	
AQUELLO		CIENT	
AQUELLO		CIERTO	
AQUI		CIERTO	
ARMADA		CINCO	
ARMAS		CIUDAD	
ASI		COLUNESES	
ASI MISMO		COMO	
AUN		CON	
AUNQUE		CONTRA	
AVEMOS		COSA	
AVER		CREE	
AVIA		CREO	
AVIENDO		DAÑO	
AYUDA		DAR	
BARON		DE	
BIEN		DE LA	
BUENA		DE LO	
BUENO		DE LO	
CAPITAN		DECIR	
CAPITANIA		DEL	


SISTEMA DE CIFRA

CÓDIGO

MARQUES		NUESTRO	
MAS		NUEVA	
MAS		O	
MAYO		OBRA	
MAYORMENTE		OFICIO	
MEJOR		OMBRES	
MERCED		ONRRA	
MI?		ORDEN	
MILAN		OTRA	
MUCHA		OTRO	
MUCHO		PAPA	
MUCHO		PARA	
MUY		PARA QUE	
NAPOLES		PARA QUE	
NAVIO		PARECE	
NECESIDAD		PARTE	
NEGOCIACION		PERO	
NEGOCIO		PERSONAS	
NI		PLACER	
NINGUNA		POR	
NINGUNA		POR QUE	
NINGUNO		PRESA	
NO		PRESO	
NO		PRUDENCIA	
NO PUEDE		PUEBLO	
NOS		PUEDE	
NOS		QUAL	
NUESTRA		QUANDO	
NUESTRO		QUANTA	
NUESTRO		QUANTO	


SISTEMA DE CIFRA

CÓDIGO

MARQUES		NUESTRO	
MAS		NUEVA	
MAS		O	
MAYO		OBRA	
MAYORMENTE		OFICIO	
MEJOR		OMBRES	
MERCED		ONRRA	
MI?		ORDEN	
MILAN		OTRA	
MUCHA		OTRO	
MUCHO		PAPA	
MUCHO		PARA	
MUY		PARA QUE	
NAPOLES		PARA QUE	
NAVIO		PARECE	
NECESIDAD		PARTE	
NEGOCIACION		PERO	
NEGOCIO		PERSONAS	
NI		PLACER	
NINGUNA		POR	
NINGUNA		POR QUE	
NINGUNO		PRESA	
NO		PRESO	
NO		PRUDENCIA	
NO PUEDE		PUEBLO	
NOS		PUEDE	
NOS		QUAL	
NUESTRA		QUANDO	
NUESTRO		QUANTA	
NUESTRO		QUANTO	

Bibliografía

Bacon, F. (1988). *El avance del saber.* ALIANZA EDITORIAL.

Carta de Juan Andrea Doria, príncipe de Melfi, a Felipe II, rey de España, sobre la entrega de nueva cifra general. (20 de julio de 1594). Obtenido de Portal de Archivos Españoles: http://pares.mcu.es/ParesBusquedas/servlets/Control_servlet?accion=3&txt_id_desc_ud=3560904&fromagenda=N

Códigos secretos en la Primera Guerra Mundial. (11 de marzo de 2015). Obtenido de Cuaderno de Cultura Científica: https://culturacientifica.com/2015/03/11/codigos-secretos-en-la-primera-guerramundial/

Criptografía en la Biblia. (5 de agosto de 2014). Obtenido de KORANET: https://koranets.net/criptografia-en-labiblia/

Criptohistoria. (s.f.). *La rejilla. Historia de un instrumento de cifrad.* Obtenido de Criptohistoria: http://www.criptohistoria.es/files/rejilla.pdf

Cuaderno de notas del Observatorio. (s.f.). *LA CRIPTOGRAFÍA DESDE LA ANTIGUA GRECIA HASTA LA MÁQUINA ENIGMA.* Obtenido de Instituto Nacional de Tecnologías de la Comunicación: http://www.egov.ufsc.br/portal/sites/default/files/la_criptografia_desde_la_antigua_grecia_hasta_la_maquina_enigma1.pdf

Daniel, C. M., Armando, F. F., & Omar, R. J. (s.f.). *U.N.A.M Criptografía.* Obtenido de https://unamcriptografia.wordpress.com/

Dávila Muro, J. (2008). *Criptografía y Seguridad: La ocultación en los textos sagrados.* Obtenido de http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-4.pdf

El Paraíso de las Matemáticas. (s.f.). *El cifrado ADFGVX*. Obtenido de El Paraíso de las Matemáticas: http://paraisomat.ii.uned.es/paraiso/cripto.php?id=adfgvx

Fernández, S. (2004). La criptografía clásica. *Sigma*(24).

García Larragan, M. (14 de octubre de 2016). *Criptografía (XXXIII): cifrado cinta móvil (I)*. Obtenido de manQiT gestión: http://mikelgarcialarragan.blogspot.com/2016/10/criptografia-xxxiii-cifrado-cinta-movil.html

GUERRA CIVIL EN ESPAÑA. (s.f.). Obtenido de donQuijote: https://www.donquijote.org/es/cultura-espanola/historia/guerra-civil/

Guerra Civil Española. (s.f.). Obtenido de Historia de España: https://historiaespana.es/edad-contemporanea/guerra-civil-espanola

Gutiérrez, Á. (s.f.). Criptografía y criptoanálisis en las dos guerras mundiales. *ACTA*.

Kahn, D. (1967). *The codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.*

LinotYpE. (s.f.). *FUENTES HEBREAS*. Obtenido de LinotYpE: https://www.linotype.com/es/6782/hebreo.html

Marcos Rivas, J. (15 de septiembre de 2014). *LA CRIPTOGRAFIA Y LOS DOCUMENTOS SECRETOS DE FELIPE II.* Obtenido de Archivo de la Frontera: http://www.archivodelafrontera.com/wp-content/uploads/2014/09/La-criptograf%C3%ADa-y-los-servicios-secretos-de-Felipe-II-por-Javier-Marcos-Rivas-11.pdf

Martí, P. (26 de diciembre de 2016). Así eran los 'mails' encriptados de Felipe II. *LA VANGUARDIA*. Obtenido de LA VANGUARDIA: https://www.lavanguardia.com/cultura/20161226/412829983932/mensajes-encriptados-felipe-ii.html

Martín San Roque, C. (11 de mayo de 2018). *¿SABÍAS QUE? CARTAS CIFRADAS DURANTE EL REINADO DE FELIPE II*. Obtenido de BLOG EL SALóN DE CRIS: https://elsalondecris.blogspot.com/2018/05/sabias-que-cartas-cifradas-durante-el.html

Moya, J. (1975). *Biblia de Jerusalén.* Desclée de Brouwer-Mensajero.

Nacio, I. (s.f.).

P, R. (8 de mayo de 2012). *Felipe II, François Viète y el diablo*. Obtenido de Ciencia y Mucho Más: https://sites.google.com/site/cienciaymuchomas/home/articulos/felipeiifrancoisvieteyeldiablo

Quirantes Sierra, A. (s.f.). *La Cifra General de Felipe II*. Obtenido de Taller de Criptografía: https://www.ugr.es/~aquiran/cripto/museo/felipeii-1556.htm

Secretos en el aire. La criptografía en la guerra civil española. (27 de noviembre de 2012). Obtenido de SCRIBD: https://es.scribd.com/document/114665016/Secretos-en-el-aire-La-criptografia-en-la-guerra-civil-espanola

Singh, S. (2000). *The code book: Science of Secrecy.* Debate.

Soler Fuensanta, J. R. (s.f.). *La Criptología Española hasta el final de la Guerra Civil.* Obtenido de DOCPLAYER: https://docplayer.es/13097526-La-criptologia-espanola-hasta-el-final-de-la-guerra-civil-jose-ramon-soler-fuensanta.html

Soriano de la Cámara, J. M. (s.f.). *CRIPTOANÁLISIS, MEDIANTE ALGORITMOS GENÉTICOS, DE TEXTOS CIFRADOS EN LA GUERRA CIVIL ESPAÑOLA CON LA TÉCNICA DE CINTA MÓVIL.* Obtenido de Instituto de Investigación Tecnológica. Comillas, Universidad Pontificia: https://www.iit.comillas.edu/pfc/resumenes/4e654ebbe0391.pdf

Suetonio. (1978). *Vida de los doce Césares.* Barcelona: Juventud.

Tabara Carbajo, J. L. (s.f.). *Criptografía Clásica.* Obtenido de GitBooks: https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto13.html

Tixaire, A. G. (s.f.). *EL ARTE DE DISFRAZAR LA INFORMACIÓN: DE LA C A LA Q.* Obtenido de Real Academia de Ciencias: http://www.rac.es/ficheros/doc/00609.pdf

Xifré Solana, P. (2008). *Antecedentes y perspectivas de estudio.* Obtenido de Universidad Carlos III de Madrid Biblioteca E-Archivo: https://e-archivo.uc3m.es/bitstream/handle/10016/6173/PFC_Patricia_Xifre_Solana.pdf?sequence=1