

UNIVERSIDAD NACIONAL DE LA MATANZA



***Departamento de Ingeniería e Investigaciones
Tecnológicas***

Seguridad y Calidad en Aplicaciones Web

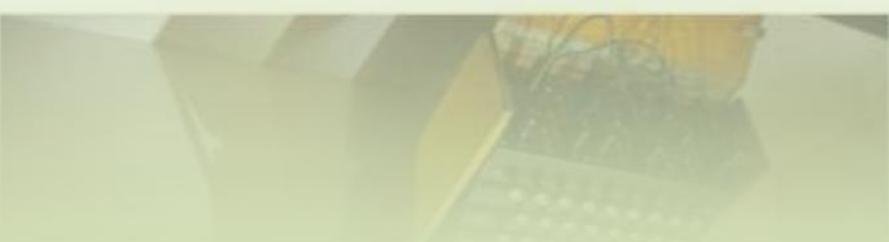
Unidad N° 3: Anexo La Máquina Enigma y otros dispositivos de encriptación

Fuente: “La Máquina Enigma y otros dispositivos de encriptación”, Germán Fco. Martínez Navarro .

La Máquina Enigma

y otros dispositivos de encriptación

Germán Fco. Martínez Navarro



1 - Sistemas de codificación antiguos	3
1.1 - Escítala	3
1.2 - Disco de Alberti (1466)	4
1.3 - Disco, rueda o cilindro de Jefferson (1795)	7
1.4 - Disco de Wheatstone (1817)	10
2 - Sistemas de codificación modernos	13
2.1 - Máquina de rotores	13
2.2 - Máquina Enigma (1923).....	14
2.3 – Typex (1937)	18
2.4 – SIGABA	19
3 – Criptoanálisis	21
3.1 - Disco de Alberti.....	21
3.2 - Disco, rueda o cilindro de Jefferson	21
3.3 - Máquina Enigma	21
4 - Acontecimientos históricos	24
A – Anexo	30
B – Bibliografía	32

1 - Sistemas de codificación antiguos

1.1 – Escítala

Una **escítala** es un sistema de codificación utilizado por los éforos espartanos para el envío de mensajes secretos. Está formada por dos varas de grosor variable y una tira de cuero o papiro, a las que ambas se puede denominar escítala.

El sistema consistía en dos varas del mismo grosor que se entregaban a los participantes de la comunicación. Para enviar un mensaje se enrollaba una cinta de forma espiral a uno de los bastones y se escribía el mensaje longitudinalmente, de forma que en cada vuelta de cinta apareciese una letra de cada vez. Una vez escrito el mensaje, se desenrollaba la cinta y se enviaba al receptor, que sólo tenía que enrollarla a la vara gemela para leer el mensaje original.



Ilustración 1: Escítala

Por ejemplo, si tenemos el siguiente mensaje:

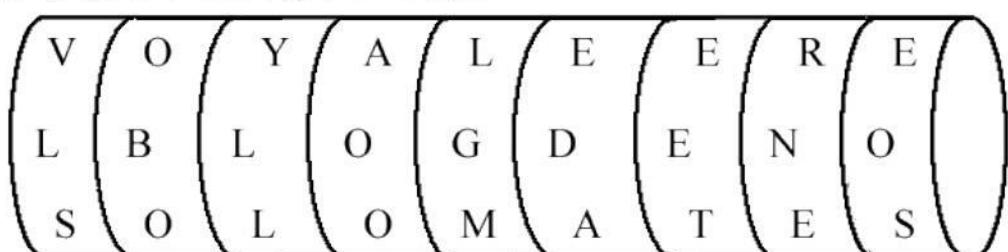


Ilustración 2: Ejemplo de encriptación mediante la escítala

Al desenrollar la cinta lo que se verá será:

VLSOBOYLLAOOLGMEDAEETRNEEOS.

En el siguiente enlace se dispone de una aplicación para ver el funcionamiento con el mensaje deseado:

<http://www22.brinkster.com/nosolomates/ayuda/cripto/criptoscitala.htm>

1.2 – Disco de Alberti (1466)

En 1466, León Battista Alberti, músico, pintor, escritor y arquitecto, concibió el primer sistema polialfabético que se conoce, que emplea varios abecedarios, utilizando uno u otro cada tres o cuatro palabras. El emisor y el destinatario habían de ponerse de acuerdo para fijar la posición relativa de dos círculos concéntricos, que determinara la correspondencia de los signos.



Ilustración 3: Alberti (1402- 1472)

Un modo práctico de implementar un **cifrado polialfabético** es el uso a tal efecto de artilugios conocidos como “**discos de Alberti**”. Estos cifradores portátiles consisten de un armazón fijo en el que está grabado un alfabeto convencional, y unido a él una pieza circular concéntrica y móvil con otro alfabeto grabado. El emisor puede, mediante el giro del anillo móvil, emparejar el alfabeto llano con tantos alfabetos cifrados como giros distintos del anillo dé, hasta un máximo igual a los caracteres del alfabeto empleado. El cifrado obtenido por un disco de Alberti es muy resistente al **análisis de frecuencias**. Para poder desencriptar el mensaje el receptor sólo necesita realizar los mismo giros que el emisor. La seguridad de este cifrado, como del resto, depende de mantener secretas las claves, esto es, el orden del alfabeto del anillo móvil más los giros realizados. Un disco de Alberti con un solo anillo móvil grabado con un alfabeto ordenado de manera tradicional permite un **cifrado César** por giro (el alfabeto interno está desordenado por este motivo).

El **disco de Alberti** presenta en su círculo exterior los 20 caracteres del latín en mayúscula, esto es, los mismos del alfabeto castellano excepto las letras H, J, Ñ, K, U, W e Y, y se incluyen los números 1, 2, 3 y 4 para códigos especiales. Por su parte, en el disco interior aparecen todos los caracteres del latín en minúscula además del signo & y las letras H, K e Y (este alfabeto es el que se encuentra desordenado). Al ser 24 los caracteres representados en cada disco, es posible definir hasta 24 sustituciones diferentes; es decir, dependiendo de la posición del disco interior la cantidad máxima de alfabetos de cifrado es igual a 24.



Ilustración 4: Disco de Alberti (1466)

Sea el disco exterior (el fijo) el texto plano y el interior (el móvil) el texto cifrado. Para encriptar hay dos métodos.

Primer método:

Se elige una letra del disco central como índice, únicamente conocido por el emisor y el receptor. En la *Iustración 4* se tiene que la letra ‘g’ ha sido elegida como índice, y se hace coincidir con la letra del disco exterior ‘A’. Los alfabetos que se tienen de esta manera son:

Exterior	A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
Interior	g	k	l	n	p	r	t	u	z	&	x	y	s	o	m	q	i	h	f	d	b	a	c	e

Supóngase que se desea cifrar el siguiente mensaje:

“La guerra si farà”

Si se emplean dos alfabetos distintos, se podría obtener algo como:

Mensaje	_	L	A	G	V	E	R	2	R	A	_
Mensaje cifrado	A	z	g	t	h	p	m	a	m	g	Q

La letra ‘A’ que aparece al inicio del mensaje cifrado indica con qué letra del disco exterior se ha de relacionar el índice. Una vez se descifra el mensaje, el ‘2’, resultado de descifrar la ‘a’, se considera un carácter nulo, por lo que se desecha. A partir de la última letra de “guerra”, se decide cambiar de alfabeto codificador; en este caso es la ‘Q’ la que pasa a emparejarse ahora con el índice ‘g’, con lo que los alfabetos que quedan ahora son:

Exterior	Q	R	S	T	V	X	Z	1	2	3	4	A	B	C	D	E	G	G	I	L	M	N	O	P
Interior	g	k	l	n	p	r	t	u	z	&	x	y	s	o	m	q	i	h	f	d	b	a	c	e

Partiendo de estos dos alfabetos, el resto del mensaje quedará:

Mensaje	_	S	I	F	A	R	À
Mensaje cifrado	Q	l	f	i	y	k	y

En resumen, lo que se tendrá será:

Mensaje	_	L	A	G	V	E	R	2	R	A	_	S	I	F	A	R	À
Mensaje cifrado	A	z	g	t	h	p	m	a	m	g	Q	l	f	i	y	k	y

Segundo método:

Se elige una letra del disco externo como índice, únicamente conocido por el emisor y el receptor. En este caso se tomará la letra ‘A’ como índice y se emparejará con la letra ‘m’. Los cambios de alfabetos se indican encriptando uno de los cuatro números. Inicialmente se tendrán los siguientes alfabetos:

Exterior	A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
Interior	m	q	i	h	f	d	b	a	c	e	g	k	l	n	p	r	t	u	z	&	x	y	s	o

El mismo mensaje de antes esta vez quedará:

Mensaje	_	L	A	G	V	E	R	A	3
Mensaje cifrado	m	c	m	b	u	f	p	m	s

En este caso, una de las dos ‘R’ se ha omitido a la hora de encriptar el mensaje. Al descifrar el mensaje, se comprueba que la letra ‘s’ coincide con el ‘3’ en el mensaje original, lo que significa que hay que mover el disco interior, concretamente la ‘s’ debe coincidir con el índice, es decir, la ‘A’. Una vez hecho esto, los alfabetos que se tienen son:

Exterior	A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
Interior	s	o	m	q	i	h	f	d	b	a	c	e	g	k	l	n	p	r	t	u	z	&	x	y

El resto del mensaje quedará cifrado como:

Mensaje	_	S	I	F	A	R	À
Mensaje cifrado	s	n	d	h	s	l	s

El cifrado resultante será:

Mensaje	_	L	A	G	V	E	R	A	A	S	I	F	A	R	À
Mensaje cifrado	m	c	m	b	u	f	p	m	s	n	d	h	s	l	s



Ilustración 5: Imagen real de un Disco de Alberti
(alfabeto actual)

En el siguiente enlace se dispone de una aplicación para realizar cifrados, pero con un único giro del disco:

<http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRYPTOGRAFIA/POLIALFABETICAS/alberti.htm>

1.3 – Disco, rueda o cilindro de Jefferson (1795)

Inventado originalmente por Thomas Jefferson (1743 - 1826), autor de la Declaración de Independencia de EEUU. Este aparato consiste en una serie de discos, originalmente 26, cilíndricos de igual diámetro que giran independientemente alrededor de un mismo eje. En el canto de cada disco están escritas todas las letras del abecedario, pero en cada una de ellos en orden distinto. De esta manera se consigue un **cifrado polialfabético**.

Para codificar los mensajes el emisor no tenía más que colocar los cilindros en orden formando el mensaje deseado, dejar inmóviles los mismos para que no se desplazasen y leer en cualquiera de sus restantes líneas la palabra resultante ya codificada, y esa línea era la que se comunicaba al receptor. El receptor del mensaje encriptado debía disponer de un cilindro similar idéntico tanto en el número de discos rotatorios como en la disposición de las letras sobre ellos, girarlos hasta formar la primera palabra codificada y leer todas las líneas hasta encontrar un mensaje que tuviese sentido.



Ilustración 6:
Thomas Jefferson
(1743-1826)

El invento, sin embargo, volvería a la vida cuando el francés Etienne Bazeries lo modificó levemente y lo puso en circulación en 1891 con el nombre de **Cilindro Bazeries**: el dispositivo constaba de entre 20 y 30 discos distintos con sus letras grabadas lo que permitía codificar frases de mayor longitud (hasta 30 letras a la vez).

Desde 1923 hasta 1942, el ejército estadounidense utilizó un cilindro de Jefferson para cifrar sus mensajes. Se llamó **M-94**, y consistía de 26 cilindros.

La Marina de los EE.UU. también hizo uso de este dispositivo bajo el nombre de código CSP488.

Ilustración 7:
Étienne Bazeries
(1846-1931)

Una característica muy importante de este sistema es que el cifrado no es determinista, el emisor puede elegir cualquier fila como mensaje cifrado.



Ilustración 8: M-94

Ilustración 9: Cilindro de Jefferson

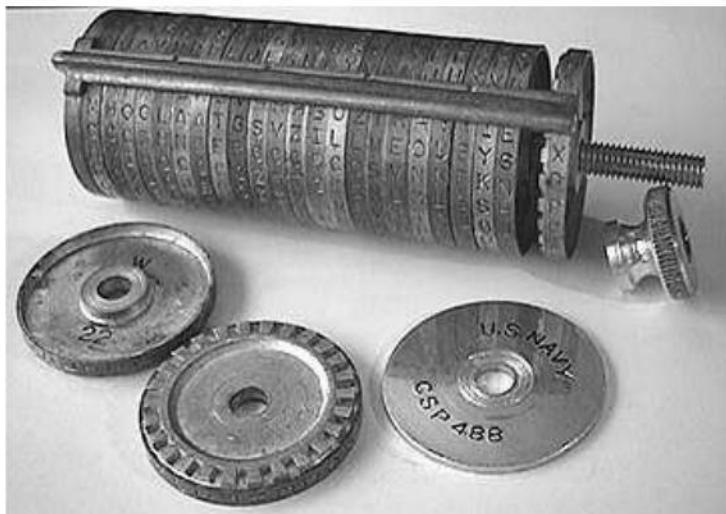


Ilustración 10: CSP 488

Supóngase que se desea encriptar el mensaje:
THOMAS JEFFERSON WHEEL CIPHER

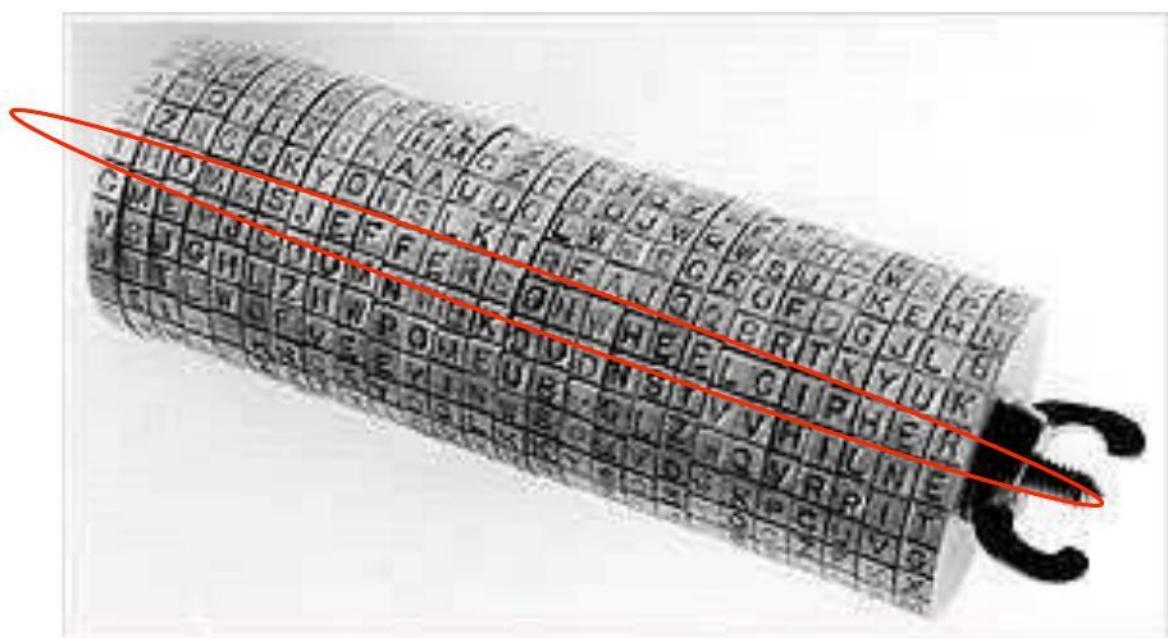


Ilustración 11: Mensaje original

Una vez dispuesta la frase en el cilindro, el emisor escoge cualquier otra línea y la envía al destinatario. Tómese como ejemplo la línea inmediatamente por encima del mensaje claro. En este caso, el mensaje cifrado enviada sería:

MZNCSK YONSLKTRF AJQQB RTXYUK

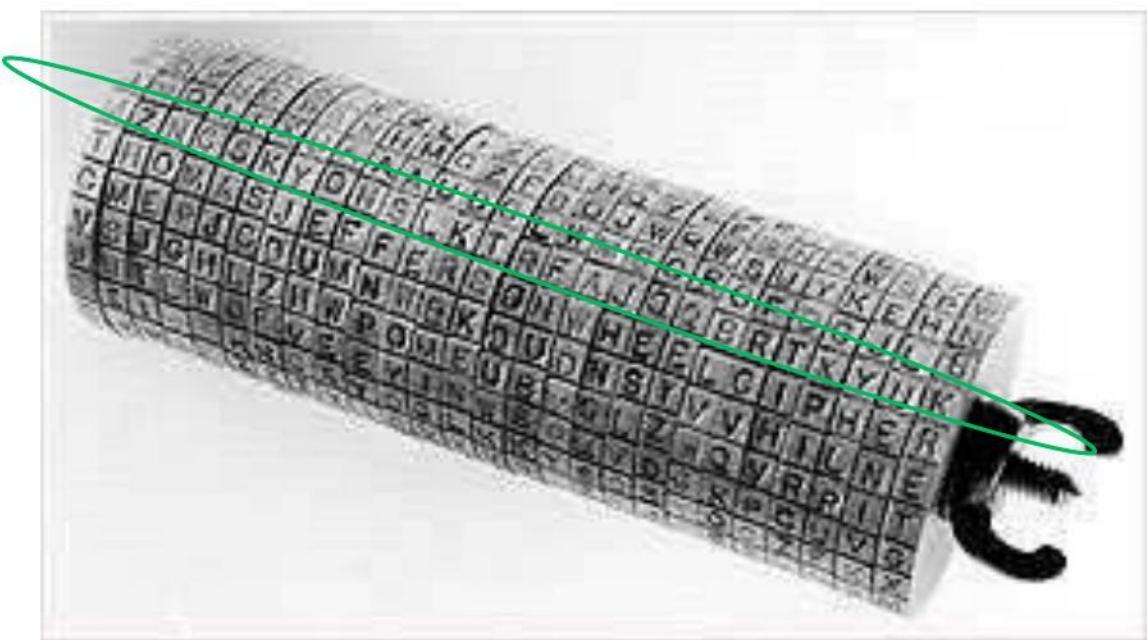


Ilustración 12: Mensaje encriptado

El destinatario, que posee un cilindro con la misma secuencia de discos, transfiere el mensaje recibido para su cilindro y busca una línea que posea texto que tenga sentido. En este ejemplo, se encuentra el mensaje descifrado en la línea inmediatamente inferior a la del mensaje cifrado.

En el siguiente enlace se dispone de una aplicación para realizar cifrados, pero con un único giro del disco:

[http://serdis.dis.ulpgc.es/~ii-
cript/PAGINA%20WEB%20CLASICA/CRYPTOGRAFIA/jefferson.htm](http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRYPTOGRAFIA/jefferson.htm)

1.4 – Disco de Wheatstone (1817)

El disco de Wheatstone, inventado por Decius Wadsworth en 1817, sigue, básicamente, el mismo algoritmo de encriptación que el disco de Alberti (sustitución polialfabética). Ahora bien, en este caso se utiliza el alfabeto inglés de 26 caracteres más el espacio en blanco para el texto en claro, representado de forma ordenada en el disco exterior, en tanto que el disco interior contiene solamente los 26 caracteres del lenguaje distribuidos aleatoriamente. Las agujas están engranadas de forma que cuando la externa gira 27 posiciones, la interna lo hace 26.



Ilustración 13: Disco de Wheatstone



Ilustración 14:
Charles
Wheatstone (1802-
1875)

Este sistema criptográfico se conoce con el nombre de disco de Wheatstone debido a que el científico e inventor inglés Sir Charles Wheatstone (1802–1875), bien conocido por el famoso **ponte de Wheatstone**, fabricó un dispositivo similar que se llevó toda la fama y la gloria (algo parecido a lo ocurrido con la rueda de Jefferson, fue Decius Wadsworth de quien surgió el modelo original, pero Charles Wheatstone fue quien lo re-inventó y se llevó la gloria).

Obsérvese que por la relación de giro de las agujas, éstas se van separando una posición o letra por cada vuelta, de forma que el alfabeto de cifrado será diferente cuando se cumpla cualquiera de estas tres condiciones:

- Que se termine una palabra del texto en claro y por tanto demos un giro completo de la aguja mayor al buscar el espacio en blanco.
- Que aparezcan letras repetidas y tengamos que dar toda una vuelta completa al buscar la segunda. No obstante, según los autores, en este caso es posible también omitir cifrar la letra repetida o bien cifrar ambas como una única letra poco usual, por ejemplo la letra Q.
- Que las letras de una palabra no vengan en orden alfabético. Es decir, si ciframos la palabra *CELOS* no alcanzamos a dar la vuelta completa al disco exterior, en tanto que la palabra *MUJER* implica dos vueltas y *HOMBRE* significa tres. La importancia de este cifrador está en que cada una de las palabras del mensaje influye en la forma en que se cifran las siguientes, una propiedad muy interesante y que precisamente utilizarán los cifradores modernos, sencillamente definiendo el concepto de palabra como bloque de bits para la cifra y aplicando lo que se denomina cifrado con encadenamiento.

Por ejemplo, partiendo del siguiente disco:

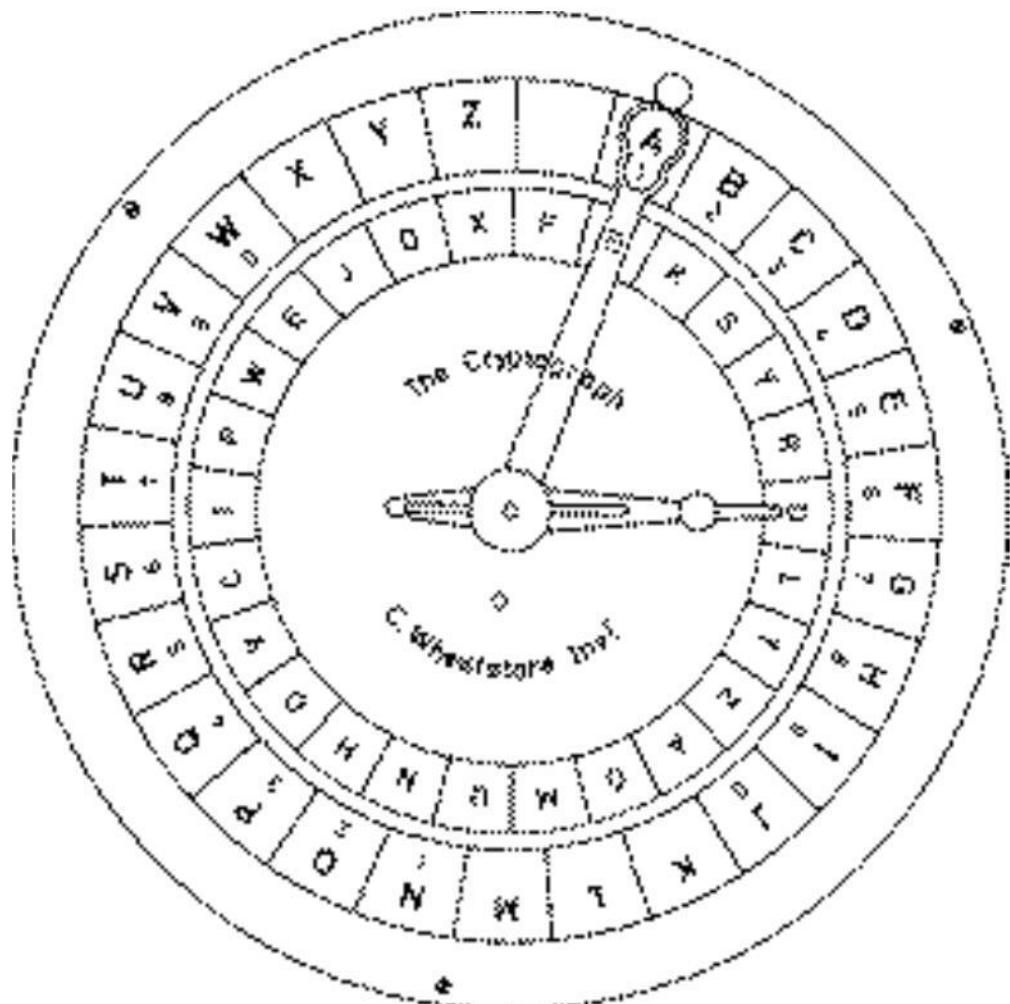


Ilustración 15: Disco de Wheatstone

Un posible cifrado para dos frases tan parecidas como las siguientes,

M_1 = CHICA FELIZ.

M_2 = CHICO FELIZ.

Quedaría:

C_1 = TUNZT T NNWIA.

C_2 = TUNZW L UUPCZ.

Como se observa en el ejemplo anterior, ambos criptogramas presentan los cuatro primeros caracteres iguales pues en el texto en claro de M_1 y M_2 también son iguales (CHIC). No obstante, la diferencia en el quinto carácter de los textos M_1 y M_2 , hace que los criptogramas resultantes a partir de ese punto sean completamente diferentes, comprobándose así la afirmación de que cada palabra influye en el cifrado de la siguiente.

Observe, además, que la primera letra C del texto en claro en ambos casos se cifra como T, en tanto que la segunda vez que aparece se cifra como Z, precisamente un espacio hacia delante en el disco interior. Esto es debido al giro completo que se produce en la operación de cifra luego de cifrar los caracteres C, H e I. Por otra parte, los caracteres repetidos TTNN en C1 y UU en C2 se deben a una revolución completa del disco interior producida por dos caracteres contiguos en el texto en claro y que están separados 26 espacios como es el caso de los diagramas "A" y "FE". Por último, apréciese que una misma palabra repetida en el texto en claro se cifrará cada

vez con un alfabeto distinto por la rotación completa producida por la búsqueda del espacio en blanco.

Por ejemplo el mensaje $M = TORA\ TORA$, palabra secreta usada como clave por los japoneses en el ataque a Pearl Harbor y cuyo significado es tigre, se cifrará como $C = XWQT\ Z\ KQBG$.

2 - Sistemas de codificación modernos

2.1 – Máquina de rotores

En criptografía, una máquina de rotores es un dispositivo electromecánico usado para el encriptar mensajes secretos. Las máquinas de rotor eran el mecanismo más importante de cifrado durante los años 30-50. El ejemplo más famoso es **Máquina Enigma**.

El componente primario es un sistema de rotores, también llamado ruedas o tambores, que son los discos que giran sobre un eje, gracias a unos contactos eléctricos en los extremos del mismo. Estos impulsos eléctricos provocan que las letras vayan cambiando de una manera compleja. De esta manera la seguridad era mínima, pero después de encriptar cada letra, el rotor volvía a avanzar, cambiando el alfabeto por el que se realizaba la sustitución. De esta manera, una máquina de rotores produce una compleja sustitución polialfabética.



Ilustración 16: Rotores

El invento de la máquina de rotores no puede atribuirse a una sola persona, ya que se le ocurrió a una serie de inventores, sin relación alguna entre ellos, al mismo tiempo.

Durante Segunda Guerra Mundial (WWII), los alemanes y los aliados desarrollaron varias máquinas de rotores. Por el lado alemán se desarrolló la famosa **Máquina Enigma**. Por el lado aliado se desarrollaron **TypeX** (Británicos) y **SIGABA** (Americanos). Había incluso una variante japonesa, la máquina Purple, aunque no era una máquina de rotores exactamente, estaba construida alrededor de interruptores eléctricos, pero era conceptualmente similar.

Las máquinas de rotores continuaron siendo utilizadas incluso en la era del ordenador. KL-7 (ADONIS), con 8 rotores, era ampliamente utilizada por los E.E.U.U. y sus aliados desde los años 50 hasta los años 80.

Pero no fueron estas las únicas máquinas que existieron. Otras, que sólo serán nombradas, fueron:

- Combined Cipher Machine.
- Lorenz SZ 40/42.
- Siemens and Halske T52.
- Fialka.
- Hebern rotor machine.
- HX-63.
- KL-7.
- Lacida.
- M-325.
- Mercury.
- NEMA.
- OMI cryptograph.
- Portex.
- RED.
- SIGCUM.
- La familia de máquinas de Hagelin, incluidas la C-36, la C-52 la CD-57 y la M-209.
- BID/60 (Singlet).
- ...

2.2 – Máquina Enigma (1923)

Dentro del gran campo de la criptografía Enigma marca el punto de inflexión entre la criptografía clásica y la moderna, entre la de antes y la de después de la existencia del ordenador. Este es el método de cifrado que pudo hacerse con una máquina que utilizaba la corriente eléctrica pero con principios de funcionamiento mecánicos. El uso de esta máquina tuvo gran importancia en la Segunda Guerra Mundial, y después ha tenido una gran repercusión en la tecnología. Su existencia produjo avances decisivos en la tecnología que, evidentemente con muchos cambios, se han convertido en imprescindibles en la actualidad, como los ordenadores.

En el año 1923 el ingeniero alemán Arthur Scherbius patentó una máquina diseñada para facilitar las comunicaciones seguras. Su nombre, Enigma, se ha convertido en sinónimo del secreto militar y evoca imágenes de laboratorios subterráneos y máquinas de enrevesada estructura. Con toda su sofisticación, Enigma es, en esencia, una versión mejorada del disco de Alberti.

La máquina Enigma en sí era un artilugio electromagnético muy parecido a una máquina de escribir. Estaba constituido por un teclado y un tablero luminoso de 26 letras; tres rotores o modificadores, que podían permutar sus posiciones, montados sobre sendos ejes, con 26 posiciones posibles, y un clavijero, cuyo cometido era llevar a cabo un primer intercambio de letras en función del modo en que se dispusieran las clavijas.

El proceso físico de cifrado era relativamente sencillo. En primer lugar, el emisor disponía las clavijas y los rotores en una posición de salida especificada por el libro de claves que estuviera vigente en ese momento. A continuación, tecleaba la primera letras del mensaje llano y la máquina, de forma automática, generaba una letra alternativa que se mostraba en el tablero luminoso: la primera letra del mensaje cifrado.

Una vez completado este proceso, el primer rotor llevaba a cabo una rotación que lo situaba en la siguiente de sus 26 posiciones posibles. La nueva posición del modificador traía consigo un nuevo cifrado de los caracteres, y el emisor introducía entonces la segunda letras, y así sucesivamente. Para descodificar el mensaje, bastaba con introducir los caracteres cifrados en otra máquina Enigma



Ilustración 17: Arthur Scherbius (1878-1929)



Ilustración 18: Máquina Enigma

con la condición de que los parámetros de salida de esta última fueran iguales a los de la máquina con la que se había llevado a cabo la encriptación.

En el dibujo siguiente se esquematiza, de forma muy simplificada, el mecanismo de encriptación de los rotores, con una alfabeto de sólo tres letras y un rotor, por tanto, con sólo tres posiciones posibles:

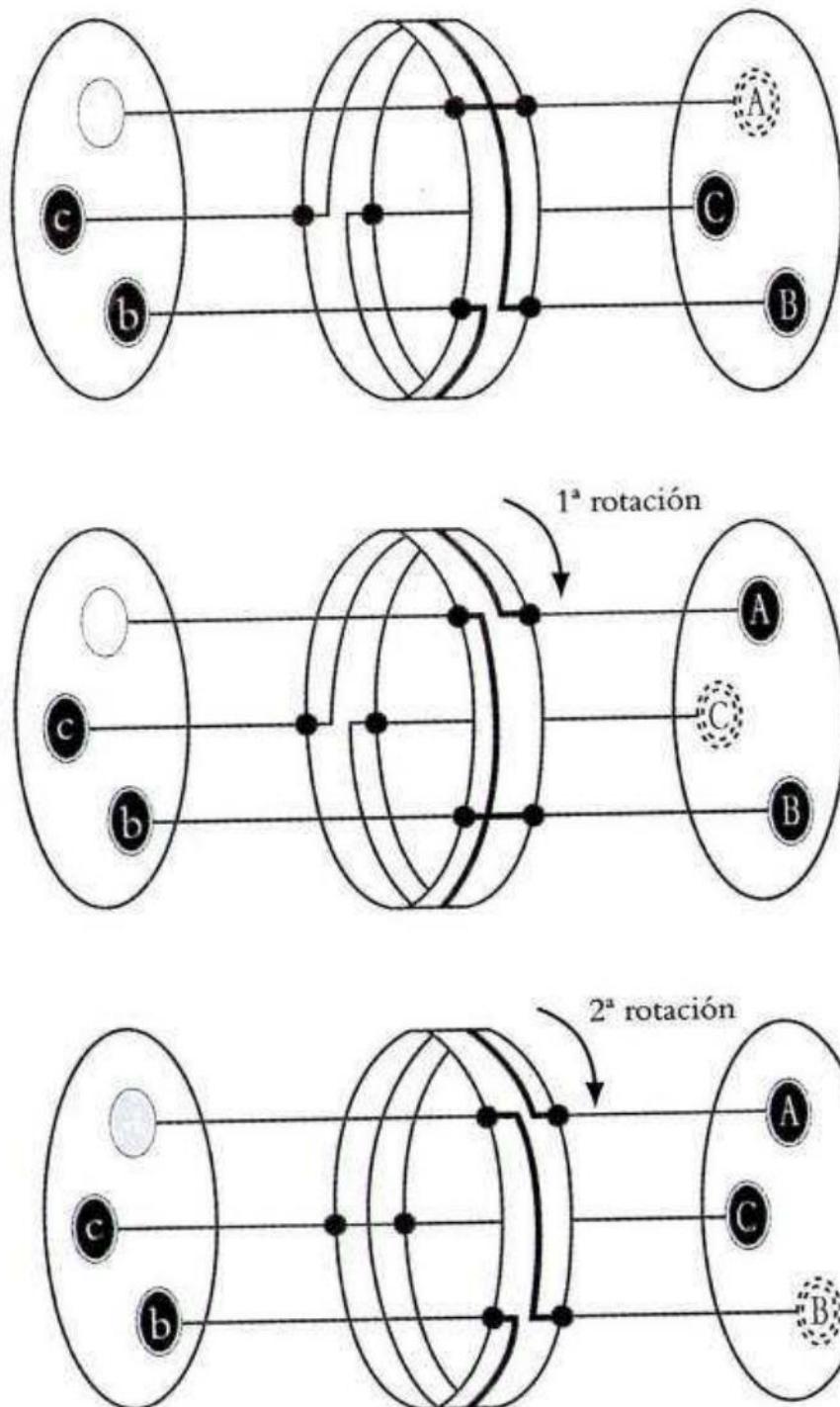


Ilustración 19: Mecanismo de encriptación de los rotores

Como puede observarse, con el rotor en la posición inicial, cada letra del mensaje original se sustituye por una distinta, excepto la A, que queda inalterada. Tras el cifrado de la primera letras, el rotor se desplaza 1/3 de vuelta. En esta nueva posición, las letras son sustituidas ahora por otras distintas a las del primer cifrado. El proceso se completa con la tercera letra, momento en el cual el rotor vuelve a su posición inicial y la secuencia de cifrado volvería a repetirse.

Como ya se ha indicado, los modificadores de la Enigma estándar tenían 26 posiciones, una para cada letra del alfabeto. En consecuencia, un modificador era capaz de llevar a cabo 26 cifrados distintos. La posición inicial del modificador era capaz de llevar a cabo 26 cifrados distintos. La posición inicial del modificador es, por tanto, la clave. Para aumentar el número de claves posibles, el diseño de Enigma incorporaba hasta tres rotores, conectados de forma mecánica uno con otro. Así, cuando el primer rotor completaba una vuelta, el siguiente iniciaba otra, y así hasta completar las rotaciones completas de los tres rotores para un total de $26 \times 26 \times 26 = 17.576$ posibles cifrados. Adicionalmente, el diseño de Scherbius permitía intercambiar el orden de los rotores, aumentando todavía más el número de claves, como veremos más adelante.

En adición a los tres rotores, Enigma disponía también de un clavijero situado entre el primero de ellos y el teclado. Este clavijero permitía intercambiar entre sí pares de letras antes de su conexión con el rotor, y añadía de este modo un número considerable de clave adicionales al cifrado. El diseño estándar de la máquina Enigma poseía seis cables, con los que se podían intercambiar hasta seis pares de letras. En el siguiente gráfico se muestra el funcionamiento del clavijero intercambiador, de nuevo con una estructura simplificada de tan sólo tres letras y tres cables:

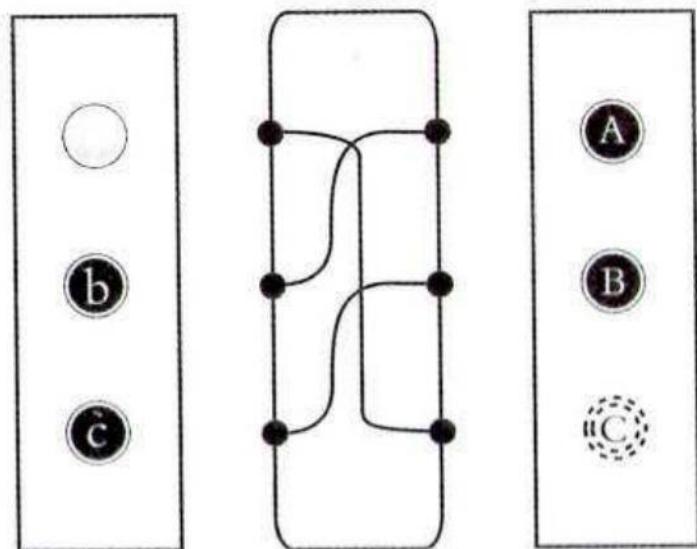


Ilustración 20: Clavijero intercambiador (simplificado)

De este modo, la A se intercambiaba con la C, la B con la A y la C con la B. Con el añadido del clavijero, una máquina Enigma simplificada de 3 letras quedaría de la siguiente manera:

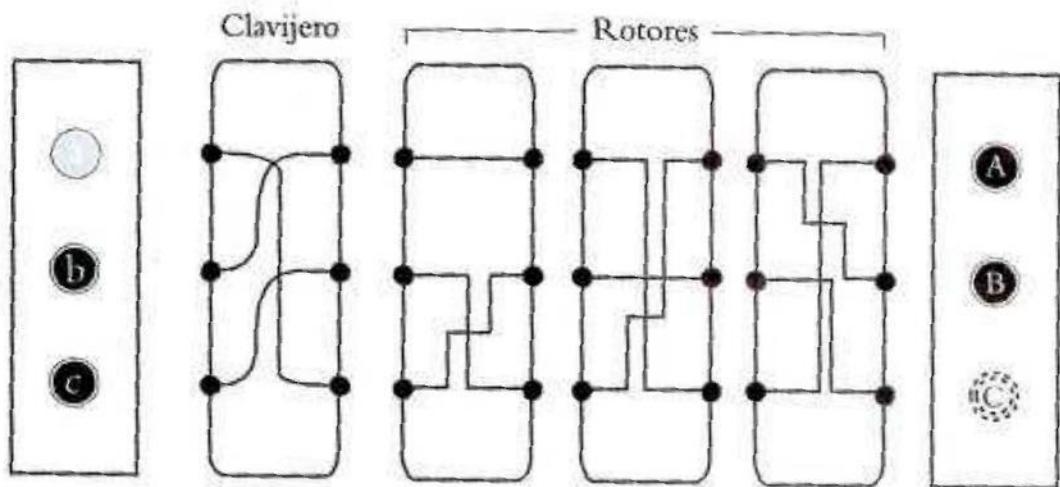


Ilustración 21: Disposición de letras en una Enigma de 3 letras

¿Qué número de claves adicionales proporcionaba el clavijero, un añadido aparentemente trivial? Hay que considerar el número de maneras de conectar 6 pares de letras escogidas entre un grupo de 26. En general, el número de posibles transformaciones de n pares de letras de un alfabeto de N caracteres viene determinado por la fórmula siguiente:

$$\frac{N!}{(N - 2n)! \cdot n! \cdot 2^n}$$

En nuestro ejemplo $N=26$ y $n=6$, de lo que resultan la friolera de 100.391.791.500 combinaciones.

En consecuencia, el número total de claves posibles que ofrece la máquina Enigma de tres rotores de 26 letras y un clavijero de seis cables es la siguiente:

1. En lo tocante a las rotaciones de los rotores, $26^3 = 26 \cdot 26 \cdot 26 = 17.576$ combinaciones.
2. Asimismo, los tres rotores (1, 2, 3) podían intercambiarse entre sí, pudiendo ocupar las posiciones 1-2-3, 1-3-2, 2-1-3, 2-3-1, 3-1-2, 3-2-1; con ello se tienen seis combinaciones posibles adicionales vinculadas, en este caso, con el orden de los modificadores.
3. Finalmente, hemos calculado que la disposición de los seis cables del clavijero inicial añadían por su parte 100.391.791.500 cifrados adicionales.

El número total de claves se obtiene del producto de las diferentes combinaciones especificadas, $6 \cdot 17.576 \cdot 100.391.791.500 = 10.586.916.764.424.000$. Por tanto, las máquinas Enigma podían cifrar un texto utilizando más de diez mil billones de combinaciones diferentes.

En el siguiente enlace se dispone de una aplicación para realizar cifrados, pero teniendo sólo en cuenta el movimiento de 3 rotores:

<http://enigmaco.de/enigma/enigma.swf>

En el siguiente enlace se pueden ver todos los modelos que existían de la máquina Enigma, con sus principales diferencias:

<http://www.cryptomuseum.com/crypto/enigma/index.htm>

2.3 – Typex (1937)

Typex fue la variante británica de la máquina Enigma, usada de 1937. Al igual que esta, Typex era una máquina de rotores, pero tenía 5, en comparación con los 3-4 que solía tener las diferentes versiones de la Enigma. Normalmente los dos primeros rotores permanecían inmóviles durante el cifrado, aunque podían ser movidos a mano. Estos dos rotores adicionales proveían a la máquina un plus de seguridad adicional similar al que las clavijas proveían a la Enigma.

Algunos rotores de Typex se dividían en dos partes: el rotor y un slug (una especie de caja donde se tenía el cableado) insertado en una carcasa de metal. Cada una de estas carcasa podían tener diferentes muescas en su borde (5, 7 ó 9). Cada slug podía ser insertado en la carcasa de dos formas: normal y dándole la vuelta. Normalmente se tenían diez slugs, de los cuales se elegían cinco.

Todas las versiones de Typex tenían una serie de ventajas sobre la máquina Enigma:

- Las máquinas Enigma requerían de dos operadores, uno para introducir el texto en la máquina y otro para copiar los caracteres ya criptografiados que se iluminaban en el panel, mientras que Typex necesitaba un único operario.
- Typex evitaba los errores producidos por el encargado de copiar a mano el texto cifrado o descifrado, ya que éste era impreso en una cinta de papel.
- A diferencia de Enigma, las Typex I estaban conectadas a **teletipos**, mientras que las Typex II lo estaban si querían.
- Los mensajes con la Enigma debían ser introducidos a mano en la máquina, encriptados por ésta, y una vez encriptados, transmitidos (por Morse). Cuando el mensaje encriptado era recibido debía ser introducido nuevamente a mano en la máquina, desencriptado por esta, y escrito a mano el resultado. Mientras que los mensajes en Typex eran impresos automáticamente ya encriptados y transmitidos (por el hecho de estar conectadas a teleimpresoras).



Ilustración 22: Máquina Typex

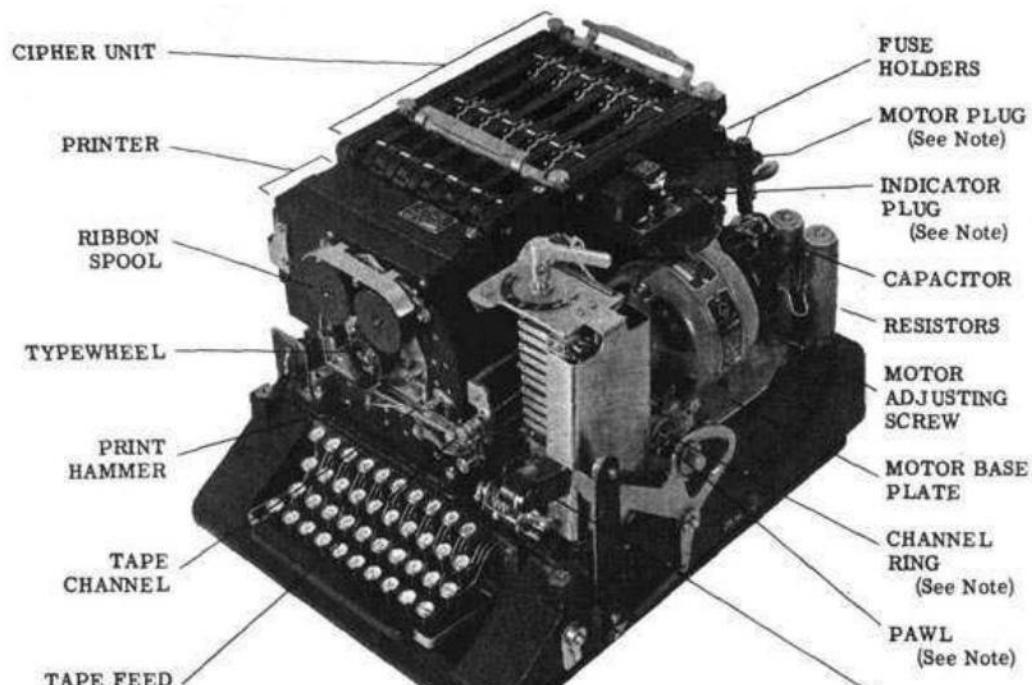
2.4 – SIGABA

SIGABA fue la variante americana de la máquina Enigma, usada durante la Segunda Guerra Mundial hasta los 50.

Básicamente, SIGABA era similar a Enigma, se basaba en una serie de rotores para encriptar los caracteres de un texto plano. Aunque la diferencia más llamativa era que SIGABA empleaba 15 rotores en vez de los 3 que usaba Enigma.

Estos 15 rotores se repartían en 3 bancos de 5 rotores cada uno; dos de esos bancos controlaban los movimientos del tercero (el banco principal):

- El banco principal era conocido como los *rotores de cifrado*, y cada uno de los 5 rotores disponían de 26 contactos. Esto es similar a lo que ocurría con Enigma, cuando una letra del texto plano era introducida, se generaba un movimiento de los rotores de manera que la letra era encriptada.
- El segundo de los bancos de 5 rotores era conocido como *rotores de control*. Cada rotor disponía también de 26 contactos. Estos rotores recibían 4 señales en cada paso. Después de pasar a través de los rotores de control, las salidas se dividían en 10 grupos de diversos tamaños, entre 1 y 6 cables. Cada grupo se correspondía con el cable de entrada al siguiente grupo de rotores.
- El tercer banco de rotores era conocido como *rotores índice*. Estos rotores eran más pequeños que los otros, y tenían sólo 10 contactos (tantos como grupos se formaban en banco anterior), que no se movían durante el procesos de encriptación. Después de atravesar este banco de rotores, sólo por entre 1 y 4 de las 5 salidas del banco circulaba corriente. Estos impulsos generados son los que llegaban al banco de *rotores de cifrado*.



Note: RING, PAWL and PLUGS
arranged for Normal Operation.

Ilustración 23: Máquina SIGABA

De esta manera SIGABA avanzaba uno o más rotores del banco principal de una compleja manera pseudoaleatoria. Esto significaba que los ataques que podían romper cualquier otra máquina de rotores con simples movimientos (como la Enigma), eran prácticamente inútiles contra SIGABA.

Pero también tenía una serie de desventajas que provocaron que no fuese tan cómoda de usar. La máquina SIGABA era grande, pesada, cara, difícil de manejar y mecánicamente compleja y frágil.

Debido a su gran serie de desventajas, SIGABA fue adaptada para interoperar con la máquina británica Typex. A esta unión se le conoció como **Máquina Combinada de la Cifra**, y fue usada a partir de noviembre de 1943.



Ilustración 24: Enigma & SIGABA

3 – Criptoanálisis

3.1 – Disco de Alberti

En su época, la cifra de Alberti era imposible de romper sin el conocimiento del método. Debido a que la distribución de las letras era aleatoria y constantemente variable el análisis de frecuencia, la única técnica sabida para atacar códigos en aquel momento, no era ninguna ayuda.

3.2 - Disco, rueda o cilindro de Jefferson

Jefferson utilizó el mecanismo para encriptar y enviar mensajes cuando era secretario de George Washington, pero pronto dejó de utilizarlo ya que su debilidad radicaba en que tanto el emisor como el receptor debían disponer de cilindros idénticos, o de lo contrario sería imposible una decodificación válida.

3.3 – Máquina Enigma

Una clave cualquiera de Enigma especificaba la posición del clavijero para cada uno de los seis intercambios de letras posibles (por ejemplo, B/Z, F/Y, R/C, T/H, E/O y L/J para indicar que el primer cable intercambiaba las letras B y Z, y así sucesivamente), el orden de los rotores (como 2-3-1) y su orientación de partida (como R, V, B para indicar qué letras quedaba situada en la parte más alta). Estas indicaciones se recogían en libros de claves que a su vez eran transmitidos de forma encriptada, y podían cambiar día a día o en función de otras circunstancias, como la naturaleza del mensaje.

Para evitar repetir una misma clave a lo largo de todo un día, durante el cual podían llegar a enviarse miles de mensajes, los operadores de Enigma recurrieron a ingeniosos trucos para transmitir nuevas claves alternativas de uso restringido sin necesidad de alterar el libro de claves comunes. Así, el emisor codificaba, de acuerdo con la nueva disposición de los rotores, por ejemplo T-Y-J (para mayor seguridad, el emisor codificaba las tres indicaciones dos veces, de ahí las seis letras). A continuación, codificaba el mensaje real de acuerdo a esa nueva disposición. El receptor recibía un mensaje que no podía descifrar de acuerdo con la clave del día, pero sabía que los seis primeros caracteres de aquél era n en realidad instrucciones para disponer los rotores en otra posición. El receptor así lo hacía, manteniendo clavijero y orden de los rotores inalterados, y podía ahora desencriptar el mensaje de forma correcta.

Los aliados obtuvieron la primera información de valor relativa a Enigma en 1931 de mano de un espía alemán, Hans-Thilo Schmidt, y consistía en varios manuales para el uso práctico de la máquina. El contacto con Schmidt había sido establecido por la inteligencia polaca, que en esos años sentía ya a sus espaldas el resuello de una Alemania cada vez más belicosa. El departamento de criptoanálisis polaco, conocido como Byuro Szyfrów, se puso a trabajar con los documentos de Schmidt y se agenció para ello varios ejemplares de máquinas Enigma sustraídas a los alemanes.

Como medida novedosa por aquella época, decidió incorporar al equipo de analistas un número considerable de matemáticos. Entre ellos se encontraba un talentoso joven de 23 años, introspectivo y tímido, llamado Marian Rejewski. Éste se puso a trabajar de inmediato y concentró sus esfuerzos, precisamente, en la clave de mensaje de seis letras que antecedia a muchos de los mensajes diarios que se intercambiaban los alemanes. Rejewski sabía que las segundas tres letras de la clave eran un nuevo cifrado de las tres primeras, y sabía, por tanto, que la cuarta, quinta y sexta letra podían dar pistas sobre la rotación de los modificadores.



Ilustración 25: Hans-Thilo Schmidt (1888-1943)



Ilustración 26: Marian Rejewski (1905-1980)

De esta constatación, por ínfima que parezca, Rejewski edificó una extraordinaria red de deducciones que iba a permitir romper el código Enigma. El detalle de este proceso es muy complejo y no se va a exponer aquí, pero el hecho es que, al cabo de unos meses, Rejewski había conseguido reducir el número de claves posibles que se debían desentrañar de los diez mil billones iniciales a los “escasos” 105.456 que resultaban de las diferentes combinaciones del orden de los rotores y sus diferentes rotaciones. Para ello, Rejewski tuvo que construir un artefacto de funcionamiento similar a Enigma, conocido como **Bomba**, capaz de cotejar cualquiera de las posibles posiciones de los tres rotores

en busca de la clave diaria. En fechas tan tempranas como 1934, el Byuro Szyfrów había conseguido romper Enigma y era capaz de descifrar cualquier mensaje en un plazo de 24 horas.

Aunque los alemanes desconocían que los polacos habían penetrado la seguridad de Enigma, no por ello dejaron de incorporar mejoras a un sistema que, al cabo, llevaba ya más de una década funcionando. En 1938, los operadores de Enigma recibieron dos rotores más que añadir a las tres ubicaciones estándar y, poco después, se distribuyeron nuevos modelos de máquina con clavijeros de diez cables.

El número de claves posibles aumentó de golpe a cerca de 159 trillones. Sólo la incorporación de dos rotores más a la rotación de modificadores aumentó de 6 a 60 las posibles combinaciones en su orden; es decir, uno cualquiera de los cinco rotores dispuestos en primer lugar (5 opciones) por uno cualquiera de los cuatro rotores restantes en la segunda posición (4 opciones) por uno cualquiera de los tres rotores restantes en la tercera posición (3 opciones) = $5 * 4 * 3 = 60$. Aunque sabía cómo descifrar el código, el Byuro Szyfrów carecía de los medios necesarios para analizar secuencialmente un número 10 veces mayor de nuevas configuraciones de los rotores.

La mejora de Enigma no fue casual: Alemania había iniciado ya su agresiva expansión por Europa con la anexión de Checoslovaquia y Austria, y planeaba la invasión de Polonia. En 1939, con el conflicto ya desatado en el corazón de Europa y su país conquistado, los polacos remitieron sus máquinas Enigma y toda su información a sus aliados británicos, que en agosto de ese año decidieron concentrar y reubicar a sus dispersas unidades de criptoanálisis. El lugar escogido fue una casa señorial situada en las afueras de Londres, en una hacienda llamada Bletchley Park. Uno de los más brillantes criptoanalistas que el gobierno había incorporado al equipo de Bletchley Park era un joven matemático llamado Alan Turing. Turing era un autoridad mundial en el ámbito de la computación, por aquel entonces un campo todavía virgen y presto a nuevos y revolucionarios desarrollos. Estos conocimientos fueron clave a la hora de descifrar la mejorada Enigma.



Ilustración 27: Alan Turing (1912-1954)

Los expertos de Bletchley Park se centraron en fragmentos cortos de texto cifrado sobre los cuales tenían fundadas sospechas de cuál era su correspondencia con textos llanos. Por ejemplo, merced al trabajo de sus espías sobre el terreno, se sabía que los alemanes tenían la costumbre de transmitir un mensaje codificado acerca de las condiciones meteorológicas en varias posiciones del frente alrededor de las 6 de la tarde de todos los días. Por tanto, estaban razonablemente seguros de que un mensaje interceptado pocos minutos después de esa hora contenía la versión cifrada de textos llanos como “clima” o “lluvia”. Turing ideó un sistema eléctrico que permitía reproducir todas y cada una de las 1.054.650 combinaciones posibles de orden y posición de los tres rotores en un tiempo inferior a las 5 horas. Este sistema era

alimentado con las palabras cifradas que, por la longitud de los caracteres y otras pistas, se sospechaba que correspondían con fragmentos de texto llano como, por ejemplo, las anteriormente citadas “clima” o “lluvia”.

Supongamos que se sospechaba que el texto cifrado FGRTY fuera la versión encriptada de “clima”. Se introducía la cifra en la máquina y si existía una combinación de rotores que devolvía como resultado la palabra “clima”, los criptoanalistas sabía que habían hallado, de las claves, la correspondiente a la configuración de los modificadores. A continuación, el operario introducía el texto cifrado en una máquina Enigma real con los rotores dispuestos según la clave. Si la máquina mostraba el texto descifrado CIMAL, por ejemplo, era evidente que la parte de la clave relativa a la posición de los cables incluía la trasposición entre las letras I y L. De este modo, se obtenía la clave en su totalidad. Los secretos de Enigma salían definitivamente a la luz. En el proceso de desarrollo y refinamiento de las máquinas analíticas mencionadas, el equipo de Bletchley Park acabó desarrollando el primer prototipo de ordenador moderno de la historia, bautizado como **Colossus**.

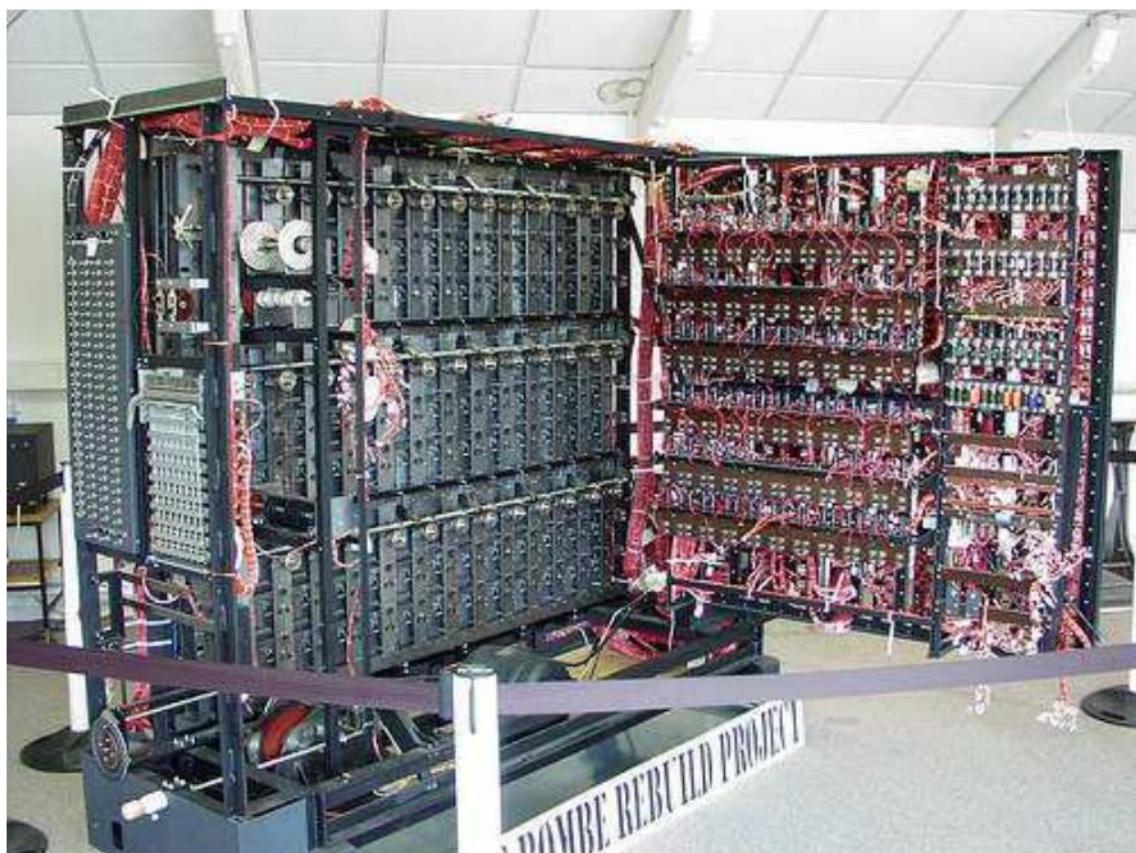


Ilustración 28:Bomba de Turing

4 – Acontecimientos históricos

Téngase en cuenta que el siguiente cuadro no es completo.

El primer texto escrito data de hace más de 6000 años. El arte del cifrado ha existido desde hace cerca de 3000 años.

c. 1900 AC	En el antiguo Egipto se usaron símbolos que no eran los normales.
c. 1500 AC	Los fenicios diseñaron un alfabeto .
c. 1000 AC	Se usaron otros símbolos distintos a los normales en la antigua Mesopotamia.
c. 600 AC	En Palestina se cifran textos usando un algoritmo simple de sustitución monoalfabética Atbash .
c. 500 AC	Los espartanos cifran mensajes utilizando Scytale .
c. 400 AC	El Kamasutra describe un algoritmo de cifrado por sustitución monoalfabética.
c. 200 AC	El historiador griego Polybius describe el cifrado de Polybius por primera vez.
c. 100-44 AC	Julio César inventa un código para cifrar sus mensajes (el Código César). Éste es el algoritmo de sustitución monoalfabética más conocido.
c.500-1400DC	La "edad oscura de la criptografía" empieza en Europa: Durante este periodo la criptografía es considerada como magia negra y se pierde gran parte del conocimiento que se tenía hasta la época. Por otro lado, la criptografía florece en Persia.
855 DC	Aparece el primer libro sobre criptografía en Arabia. Entre otras cosas, Abu 'Abd al-Raham al-Khahil ibn Ahmad ibn'Amr ibn Tammam al Farahidi al-Zadi al Yahamadi (Abu-Yusuf Ya'qub ibn Ishaq al-Kindi, conocido como Al-Kindi) describe orgulloso en su libro un mensaje griego descifrado que es deseado por el emperador bizantino. Su criptoanálisis se ha basado en un análisis de frecuencia ayudado con el conocimiento de una pequeña porción del comienzo del texto original -- este mismo criptoanálisis es el que se empleará en la Segunda Guerra Mundial contra Enigma.
1379	El papa Clemente VII ha escapado a Avignon y ha ordenado a su secretario, Gabrieli di Lavinde (Parma), diseñar un nuevo código para cifrar sus mensajes. Este código consiste en una combinación de sustituciones de letras individuales y palabras codificadas. Gabrieli ha creado una lista de las palabras más comunes que son sustituidas por combinaciones de dos letras y el resto de palabras que no están en la lista son cifradas utilizando sustitución monoalfabética. Debido a la sencillez de este código, será utilizado durante los próximos 450 años, sobre todo en los círculos diplomáticos.
1412	En Arabia se escribe una enciclopedia con 14 tomos en donde se explican conceptos de criptografía. En ella, además de las técnicas de sustitución y transposición , se explica un método consistente en repetidas sustituciones de cada carácter del texto claro. Es la primera vez en la historia que habla de un método como éste.
Siglo XV	En Italia se produce un <i>boom</i> de la criptografía debido un alto desarrollo de la vida diplomática.
1466	Leon Battista Alberti , uno de las figuras líderes del Renacimiento

	Italiano, publica su libro "Modus scribendi in ziferas", en donde habla por primera vez del disco de Alberti , el primer sistema polialfabético que se conoce. Alberti es el secretario de un cuerpo oficial perteneciente a la corte papal que se encarga únicamente de labores relacionadas con la criptografía. Por todo esto, Alberti será conocido como el "padre de la criptografía".
1518	Se imprime el primer libro sobre criptografía cuyo título es "Polygraphia libri sex", escrito por el abad Johannes Trithemius en lengua alemana. En este libro también se describen cifrados polialfabéticos con las nuevas tablas de sustitución rectangulares.
1563	Giovanni Battista Porta publica "De Furtivis Literarum Notis", un libro en el que describe distintos métodos de cifrado y criptoanálisis. En él se menciona el primer cifrado por sustitución digráfica.
Finales del s.XVI	Francia toma la delantera en criptoanálisis.
1577	El brillante criptoanalista flamenco Van Marnix cambia el rumbo de la historia europea al descifrar una carta española en donde se explicaban los planes para conquistar Inglaterra enviando tropas desde los Países Bajos.
1585	El diplomático francés Blaise de Vigenère publica su libro "Tractié de Chiffre" en donde presenta el primer sistema polialfabético con autoclave, conocido como "Le chiffre indéchiffrable" aunque más adelante se le cambiará el nombre por el de el cifrado de Vigenère . La idea de la autoclave perdurará en el tiempo y se aplicará en los algoritmos futuros como el DES en los modos CBC y CFB.
1586	Se intenta llevar a cabo el complot Babington por el cual se asesinaría a la reina Elisabeth I de Inglaterra y se colocaría en el trono a Mary Stuart, Reina de Escocia. El "Servicio Secreto Británico" pone fin a esta trama y consigue los nombres de los conspiradores, condenando a Mary Stuart. Mary se comunicaba a través de cartas con sus conspiradores. Pero el mensajero, que era un espía de Elisabeth realizaba copias exactas de cada carta y las enviaba a Francis Walsingham, secretario del estado de Elisabeth, que a través de Thomas Phelippes consiguió descifrarlas revelando el complot. Pero la cosa no quedó ahí, Walsingham quería saber la identidad de los conspiradores por lo que hizo que Phelippes añadiera una posdata a una carta, de manera que en la respuesta a la carta, Mary incluyó el nombre de los implicados.
Siglo XVII	Comienza la era de las cámaras negras . La mayoría de los gobiernos disponen de departamentos en donde profesionales se encargan de romper los cifrados a los que tienen acceso.
1623	Sir Francis Bacon describe un método de esteganografía: cada letra del texto claro es reemplazada por un grupo de cinco letras formado por una combinación de las letras 'A' y 'B' que se intercalan en un texto normal con una fuente diferente. Este método es el precursor del que luego será conocido como codificación birania de 5 bits.
1628	Antoine Rissignol se convierte en el primer criptoanalista contratado a tiempo completo tras descifrar un mensaje del enemigo gracias al cual se puso fin al sitio que los hugonotes ejercían sobre Realmont. Desde

	entonces, el papel del criptoanalista ha sido fundamental en toda organización militar.
1700	El zar de Rusia utiliza una gran tabla de códigos de 2000-3000 sílabas y palabras para cifrar sus mensajes.
1795	Thomas Jefferson diseña el primer dispositivo de cifrado cilíndrico, conocido como la "rueda de Jefferson". Sin embargo, no lo utilizará nunca, por lo que caerá en el olvido o, más bien, no se llegará a hacer público.
1854	El matemático inglés Charles Babbage inventa un dispositivo de cifrado cilíndrico similar al de Jefferson. Además, descubre un método de criptoanálisis para romper el, hasta ahora conocido, "cifrado irrompible" que diseñó Vigenère. Es por ello que a partir de este momento se conocerá como el cifrado de Vigenère, aunque en realidad esto no se hará público hasta su muerte ya en el siglo XX.
Siglo XIX	La criptología encuentra un lugar en la literatura: Arthur Conan Doyle, Julio Verne, Edgar Allan Poe...
1854	El físico inglés Charles Wheatstone inventa un cifrado que utiliza una matriz de 5x5 como clave. Su amigo, Lord Lyon Playfair, barón de Saint Andrews lo hace público en círculos militares y diplomáticos y, por ello, se conocerá como el cifrado de Playfair .
1863	Friedrich Kasiski (1805-1881), un importante prusiano, desarrolla métodos estadísticos de criptoanálisis que fueron capaces de romper el cifrado de Vigenère.
1883	Se publica "La Cryptographie militaire" de Auguste Kerckhoff von Nieuwendhoff. Esto supondrá un hito en la criptografía telegráfica de la época. Contiene el "principio de Kerckhoff", que exige basar la seguridad de un método de cifrado únicamente en la privacidad de la clave y no en el algoritmo.
1891	El francés Etienne Bazeries inventa un dispositivo cilíndrico conocido como el cilindro Bazeries que, en principio, es similar a la rueda de Jefferson. Se publicará su diseño en el año 1901, después de que el Ejército francés lo rechace.
1917	El descifrado de los telegramas de Zimmermann por el Servicio Secreto Inglés provocó la crítica entrada de los EEUU en la Primera Guerra Mundial
1917	El americano Gilbert S. Vernam , empleado de AT&T, desarrolla la cinta aleatoria de un sólo uso, el único sistema criptográfico seguro.
1918	El criptoanalista francés, Lieutenant Georges Painvin rompe el cifrado ADFGVX , que es el que usaba el ejército alemán desde un poco antes del fin de la Primera Guerra Mundial. Este algoritmo consistía en un cifrado en dos pasos; primero se realizaba una sustitución (cada letra era sustituida por un bi-grama a través de una matriz que hacía de clave) y después, los bi-gramas se dividían en columnas que se reorganizaban.
1918	Arthur Scherbius y Richard Ritter inventan la primera Enigma . Al mismo tiempo, la máquina de rotores es inventada y patentada por Alexander Koch (Países Bajos) y Arvid Damm (Suecia).
1920	William F. Friedman (1891-1969), tras ser galardonado como el padre de la criptografía estadounidense, diseña (sin relación con Kasiski) métodos estadísticos para criptoanalizar el cifrado de Vigenère.

1921	El californiano Edward Hebern construye la primera máquina de cifrado basada en el principio de los rotores
1922	La rueda de Jefferson es redescubierta en los EEUU, cuyo cuerpo de marines la rediseña y la utiliza durante la Segunda Guerra Mundial.
1923	La máquina de rotores Enigma , diseñada por el alemán Arthur Scherbius, se revela en el International Post Congress. Además, Scherbius funda la compañía "Chiffriermaschinen AG" para comercializar Enigma en todo el mundo.
1929	Lester S. Hill publica el artículo "Cryptography in an Algebraic Alphabet". El cifrado de Hill aplica álgebra (multiplicación de matrices) para cifrar.
1940	Los espías alemanes utilizan micropuntos.
1940	Alan Turing rompe Enigma con la idea de la Bomba de Turing que concibió basándose en el trabajo de Marian Rejewski .
1941	Se descifran los mensajes con los que se comunicaban los japoneses en donde se hablaba del inminente ataque a Pearl Harbor. Esto es debido a la labor de un equipo dirigido por William Frederick Friedman, que rompió la máquina japonesa Purple. Muchos historiadores creen que el criptoanálisis acortó en una año la Segunda Guerra Mundial.
1948/1949	Claude Shannon establece las bases matemáticas de la teoría de la información y publica "Communication Theory of Secrecy Systems", en donde expone un algoritmo de cifrado teóricamente irrompible que debe satisfacer los requisitos de la cinta aleatoria de un sólo uso.
1973	David Elliott Bell y Len LaPadula desarrollan el modelo Bell-LaPadula que formaliza las normas de acceso a la información clasificada, con la intención de lograr la confidencialidad de los datos.
1973-1975	Ellis, Cocks y Williamson desarrollan un algoritmo de cifrado de clave pública para el gobierno británico (GCHQ). Este descubrimiento no será conocido públicamente hasta 1997. Debido a esto, los métodos de cifrado asimétrico serán nuevamente reconstruidos de forma independiente y, esta vez sí, públicamente por Diffie, Hellman, Rivest, Shamir y Adleman, que serán considerados los descubridores de la criptografía de clave pública.
1975	Diffie y Hellman describen que los procedimientos de clave pública son teóricamente posibles, a pesar de que se ha intentado demostrar lo contrario.
1976	Whitfield Diffie y Martin Hellman publican "New Directions in Cryptography". Que introduce un nuevo método de distribución de claves criptográficas, lo que era hasta la fecha uno de los problemas fundamentales de la criptografía. Este mecanismo será conocido como el protocolo Diffie-Hellman de intercambio de claves.
1977	El algoritmo inventado por IBM en 1975, DES (Data Encryption Standard) , es elegido por el NIST (FIPS PUB-46) como el algoritmo de cifrado estándar de los EEUU.
1977	El algoritmo RSA , llamado así por sus desarrolladores, Ronald Rivest, Adi Shamir y Leonard Adleman, es publicado. RSA supone el primer procedimiento de clave pública utilizado en la práctica y ocupa el puesto de ser la contribución criptológica más innovadora del siglo XX.

1979	Los primeros cajeros automáticos (Automatic Teller Machines) utilizan DES para cifrar los códigos PIN.
1982	El físico Richard Feynman diseña el modelo teórico de una computadora cuántica .
1984	Charles H. Bennett y Gilles Brassard describen la criptografía cuántica (BB84 protocol).
1985	Goldwasser, Micali y Racoff descubren el procedimiento de conocimiento cero .
1986	De forma independiente, Neal Koblitz y Victor Miller proponen usar curvas elípticas como modelo de criptografía de clave pública.
1991	Xuejia Lai y James Massey desarrollan el algoritmo IDEA en Suiza, que será usado en el software criptográfico PGP .
1991	DSA es elegido por el NIST como algoritmo estándar de firma digital.
1991	PGP (Pretty Good Privacy) es diseñado por Phil Zimmermann como un software gratuito y de código libre, con el fin de cifrar e intercambiar archivos con una gran seguridad. Esta es la primera vez que el cifrado híbrido (combinación de criptografía simétrica y asimétrica) es aplicada a un programa popular para usuarios finales. El objetivo principal era el de cifrar los archivos adjuntos del correo electrónico (que más tarde también fue cubierto por el estándar S/MIME).
1994	Peter Shor concibe un algoritmo para ordenadores cuánticos que permite la factorización de enteros largos. Este es el primer problema interesante para el que los ordenadores cuánticos han prometido una importante aceleración, y que, por lo tanto, genera un gran interés en este tipo de ordenadores.
Agosto 1994	El protocolo de cifrado SSL 1.0 es publicado por Netscape Communications y es soportado por todos los navegadores web. No obstante, el protocolo de transporte de SSL (TLS) no se limita a la aplicación de HTTPS.
Octubre 1995	S/MIME , un mecanismo estándar para la seguridad del correo electrónico, es publicado como RFC 1847 y cuenta con el apoyo de todos los clientes de correo electrónico. S/MIME (Secure/Multipurpose Internet Mail Extensions) describe una manera consistente para enviar y recibir mensajes de correo electrónico seguros (firmados y/o cifrados). Se basa en el estándar de Internet MIME. Sin embargo, S/MIME no sólo se limita al correo. S/MIME y SSL son los protocolos criptográficos que se utilizan con mayor frecuencia en Internet.
17 de Julio de 1998	El ingenio de la EFF conocido como Deep Crack, rompe una clave DES con un ataque de texto claro conocido en 56 horas (Los RSA Laboratories lanzan el desafío DES II).
19 de Enero de 1999	Deep Crack y distributed.net rompen una clave DES con un ataque basado en texto claro conocido en 22 horas y 15 minutos (Los RSA Laboratories lanzan el desafío DES III)
Octubre 2000	Tras la competición pública que ha durado 5 años, el algoritmo Rijndael es elegido por el NIST como el sucesor de DES y pasa de denominarse AES (Advanced Encryption Standard) .
Desde el 2000	Weil Pairing es utilizada para los nuevos esquemas de compromiso como IBE (Identity Based Encryption, que resultó ser más interesante desde un

	punto de vista teórico que desde un punto de vista práctico).
Agosto 2004	En la conferencia Crypto 2004, los investigadores chinos muestran debilidades estructurales en común de las funciones de hash (MD5, SHA), lo que las hace vulnerables a ataques de colisión. Estas funciones de hash todavía se usan en casi todos los protocolos criptográficos. Los investigadores chinos no publicaron todos los detalles.
Mayo 2005	Jens Franke y otros factorizan un número RSA-200 de 663 bits de longitud.
Abril 2007	El protocolo WEP de codificación en LAN inalámbrica fue roto por tres investigadores del TU Darmstadt. Asumiendo suficiente tráfico de datos en la red, sólo se tarda unos dos minutos en obtener el 95% de todas las claves de codificación utilizadas.
Agosto 2007	En la conferencia Crypto 2007 se mostró un algoritmo para romper el sistema inmovilizador utilizado en millones de coches. Durante la presentación, Eli Biham, Orr Dunkelman, entre otros, pudieron mostrar un ejemplo donde una correspondiente llave de coche se copió en 48 horas con la potencia de computación de 50 PCs.
Agosto 2007	David Hulton y Joshua Laykey rompieron el algoritmo de codificación A5, de marca registrada, usado por muchos operadores de GSM. Esto implica que en redes móviles afectadas, incluso las más cortas llamadas de voz o los mensajes SMS pueden descifrarse fácilmente por un PC normal, mostrando así que "seguridad por oscuridad" no es un buen enfoque.
Diciembre 2007	Se descifró el algoritmo de autenticación de las tarjetas de chip Mifare , el cual se usa en miles de aplicaciones por un billón de tarjetas expedidas. Sin embargo, la última generación (Mifare DESFire), que utiliza DES/3-DES, no se ve afectada.

A – Anexo

Cifrado César: El cifrado César consiste en reasignar a cada letra del abecedario otra nueva resultante de desplazar éste un determinado número de lugares. Tal como hace constar el gran historiador Suetonio en su *Vida de los Césares*, Julio César cifraba su correspondencia particular mediante un algoritmo de sustitución de este tipo: cada letra del mensaje original era sustituida por la que le seguía tres posiciones más adelante en el alfabeto: la letra A era sustituida por la D, la B por la E, y así hasta la última letra.

En la tabla siguiente se muestra el alfabeto de partida y la transformación que realiza un cifrado César de tres posiciones adelantadas para el alfabeto español de 27 letras. En la fila superior se muestra el alfabeto original y, en la inferior, el alfabeto cifrado:

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

Análisis de frecuencias: Una manera de resolver un mensaje cifrado, si se sabe en qué lengua está escrito, es encontrar un texto llano escrito en la misma lengua, suficientemente largo, y luego contar cuantas veces aparece cada letra. A la letra que aparece con más frecuencia se le llama “primera”, a la siguiente en frecuencia se le llama “segunda”, ... y así hasta que se hayan cubierto todas las letras que aparecen en el texto. Luego se observa el texto cifrado que se quiere resolver y se clasifican sus símbolos de la misma manera. Se encuentra el símbolo que aparece con mayor frecuencia y se sustituye por la “primera” de la del texto plano, se hace lo mismo con la “segunda” y así sucesivamente, hasta que se haya cubierto todos los símbolos del criptograma que se desea resolver.

Las letras que más aparecen en textos españoles por orden de más a menos frecuente son: E A O L S N D R U I T C P M Y Q B H G F V W J Z X K. Pueden observarse los porcentajes de aparición de cada una de estas letras en la siguiente tabla de frecuencias:

A	11,96%	H	0,89%	Ñ	0,29%	U	4,80%
B	0,92%	I	4,15%	O	8,69%	V	0,39%
C	2,92%	J	0,30%	P	2,77%	W	0,01%
D	6,87%	K	0,01%	Q	1,53%	X	0,06%
E	16,78%	L	8,37%	R	4,94%	Y	1,54%
F	0,52%	M	2,12%	S	7,88%	Z	0,15%
G	0,73	N	7,01%	T	3,31%		

Cifrado polialfabético: Ideado por Leon Battista Alberti alrededor de 1460. Consistía en un sistema de encriptación que consistía en añadir al alfabeto cifrado convencional un segundo, tal como se muestra en la tabla siguiente:

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

Ilustración 29: (1) Alfabeto llano (2). Alfabeto cifrado 1. (3) Alfabeto cifrado 2.

Para encriptar un mensaje cualquiera, Alberti proponía alternar uno y otro alfabetos cifrados. Por ejemplo, para el caso de la palabra MARCA, la cifra de la primera letra se buscaría en el primer alfabeto (O), la de la segunda en el segundo (M), y así sucesivamente. En nuestro ejemplo, MARCA quedaría cifrada como OMUBD. La ventaja de este algoritmo de encriptación polialfabético, en comparación con los anteriores, es evidente a un primer vistazo: un mismo carácter de texto llano, A, queda cifrado de dos maneras distintas, M y D. Para mayor confusión de cualquier criptoanalista que se enfrentara al texto encriptado, un mismo carácter cifrado podría representar en realidad dos caracteres distintos del texto llano. El análisis de frecuencias perdía así buena parte de su utilidad.

Teletipo: Un teletipo es un dispositivo telegráfico de transmisión de datos, ya obsoleto, utilizado durante el Siglo XX para enviar y recibir mensajes mecanografiados punto a punto a través de un canal de comunicación simple, a menudo un par de cables de telégrafo.

Puente de Wheatstone: Un puente de Wheatstone es un instrumento eléctrico de medida inventado por Samuel Hunter Christie en 1832, mejorado y popularizado por Sir Charles Wheatstone en 1843. Se utiliza para medir resistencias desconocidas mediante el equilibrio de los brazos del puente. Estos están constituidos por cuatro resistencias que forman un circuito cerrado, siendo una de ellas la resistencia bajo medida.



Ilustración 31: Puente de Wheatstone

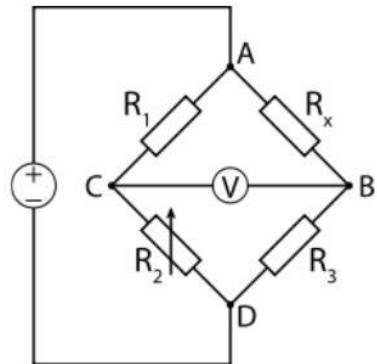


Ilustración 30: Disposición de un Puente de Wheatstone

B – Bibliografía

General:

- Matemáticos, espías y piratas informáticos. Codificación y criptografía – Joan Gómez
- <http://www.24flotilla.com/A11/otros/Historia%2520Criptografia.pdf>
- <http://www.u-historia.com/uhistoria/historia/articulos/inienigma/inienigma.htm>
- <http://www.govannom.org/seguridad/7-criptografia/439-historia-de-la-criptografia.html>
- <http://es.wikipedia.org/wiki/Teletipo>

Escítala:

- <http://www22.brinkster.com/nosolomates/ayuda/cripto/criptoscitala.htm>
- <http://es.wikipedia.org/wiki/Esc%C3%ADtala>

Disco de Alberti:

- <http://argosunois.blogspot.com/2008/04/el-disco-de-alberti.html>
- <http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRYPTOGRAFIA/POLIALFABETICAS/alberti.htm>
- http://en.wikipedia.org/wiki/Alberti_cipher_disk
- Matemáticos, espías y piratas informáticos. Codificación y criptografía – Joan Gómez

Rueda de Jefferson:

- <http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRYPTOGRAFIA/jefferson.htm>
- http://www.worldlingo.com/ma/enwiki/es/Jefferson_disk
- <http://www.sinewton.org/numeros/numeros/74/Aertura.pdf>
- http://library.thinkquest.org/07aug/01676/spanish/downtheages_wars_toolsanddevices_jeffersonswheel.html
- <http://en.wikipedia.org/wiki/M-94>
- http://en.wikipedia.org/wiki/Jefferson_disk

Disco de Wheatstone:

- <http://repositorio.bib.upct.es/dspace/bitstream/10317/110/1/pfc1724.pdf>

Máquina de rotores:

- http://en.wikipedia.org/wiki/Rotor_machine#Various_machines
- http://www.worldlingo.com/ma/enwiki/es/Rotor_machine

Máquina Enigma:

- http://www.worldlingo.com/ma/enwiki/es/Enigma_machine
- http://en.wikipedia.org/wiki/Enigma_machine
- Matemáticos, espías y piratas informáticos. Codificación y criptografía – Joan Gómez

TypeX:

- <http://www.worldlingo.com/ma/enwiki/es/TypeX>
- <http://en.wikipedia.org/wiki/TypeX>

SIGABA:

- <http://www.worldlingo.com/ma/enwiki/es/SIGABA>
- <http://en.wikipedia.org/wiki/SIGABA>

