

# Historia de la criptografía

## Índice

.....	2
Primeras fuentes.....	3
Escítala.....	3
Cifrador de Polibio.....	4
Cifrado de César.....	5
Criptoanalistas árabes.....	6
Cifrado de Battista.....	7
Cifrado de Vigenère.....	8
La Cifra General.....	11
Cifrado de Playfair.....	13
Código Morse.....	15
Kasiski y los papeles de Beale.....	16
La máquina Enigma.....	18
Cifrado ADFGVX.....	22
Principio de Kerckhoffs.....	23
DES.....	24
AES.....	28
Clave pública.....	31
Bibliografía.....	33

## Primeras fuentes

En el año 3600 a.C, los egipcios desarrollaron la escritura jeroglífica y los sumerios la cuneiforme. Sin embargo, la primera muestra de criptografía se cree que fue realizada en 1900 a.c. Se trata de un jeroglífico Egipcio, realizado mediante un grabado en piedra de un noble, en una ciudad cerca del Nilo. En este jeroglífico se muestran los actos más importantes de la vida del noble fallecido.



*Ilustración 1: Grabado de piedra en la tumba de Menet Khufu*

Analizando la muestra criptográfica, se han encontrado evidencias de que los símbolos utilizados eran diferentes a los habituales de la fecha y, lo más importante, es que había un proceso de sustitución entre ellos. Se considera la primera muestra de la criptografía a lo largo de la historia, pero también se cree que su intención no era cifrar los hechos más importantes de su vida, sino mejorar la estética del resultado final.

En 1500 a.C, aparece en Mesopotamia la primera pieza de criptografía con el fin de ocultar información. Debido a su sencillez, utilizaban un método de cifrado por sustitución. Este método es muy usado a lo largo de la criptografía pero se debe tener cuidado por su fácil fragilidad.

Aproximadamente mil años después de los cifrados mesopotámicos, nos encontramos con los cifrados hebreos. Estos cifrados también utilizan la sustitución y se consideran de gran importancia en la criptografía ya que son las primeras muestras donde se ocultaba el nombre de personas y lugares importantes.

## Escítala

En el 500 a.C. se propone en Alejandría el sistema conocido como Fryctoria, una metodología de enviar mensajes a través de antorchas. El primer método criptográfico con fines militares de la historia proviene de los espartanos en el siglo V a.C y fue utilizado en las guerras del Peloponeso (entre Esparta y Atenas) por los lacedemonios.

Consistía en un método de transposición, donde la esencia del cifrado residía en el grosor de la barra con la que se quería cifrar o descifrar. Un ejemplo de su uso lo podemos encontrar en el libro *Vidas paralelas* del historiador y filósofo griego Plutarco. Plutarco cuenta en su libro como los éforos mandaban mensajes cifrados a los comandantes de la armada. Simplemente, cortaban dos barras de madera del mismo tamaño y del mismo grosor. Cada una de estas barras recibían el nombre de correas y eran repartidas entre el emisor y receptor. En la elaboración del mensaje, utilizaban una tira de papiro larga y estrecha y la estiraban alrededor de la correa, escribiendo el mensaje de manera longitudinal. De esta forma se generaba un mensaje cifrado con letras descolocadas e inteligibles por personas.

Un ejemplo sencillo de este método consiste en utilizar como correa un lápiz hexagonal y un pedacito de folio. El folio se enrolla alrededor del lápiz y consiste en escribir a lo largo de las caras hexagonales que van desde la goma hasta la punta. Si una cara se termina, se gira un poco la correa (el lápiz) y se continúa escribiendo. El método de descifrado es igual solo que en vez de escribir se debe leer.



FIGURA 1. Escítala de los Lacedemonios (grabado de 1581)

*Ilustración 2: Escítala (1581)*



*Ilustración 3: Escítala(1581)*

## Cifrador de Polibio

Otro ejemplo de referencia y criptografía clásica se la debemos al historiador griego Polibio. El cifrador de Polibio se trata de un método por sustitución desarrollado el 120 a.C., donde para codificar el texto se debe establecer una matriz, en la que todas las letras se encuentren en una tabla mediante columnas y filas enumeradas. Básicamente consiste en una tabla de cinco filas y cinco

columnas, es decir, veinticinco posiciones. A partir de esta tabla, se puede identificar cada letra por su número de fila y columna. El algoritmo de cifrado consiste en sustituir cada letra por el par de números fila columna que describe la posición de la letra dentro de la matriz.

A pesar de su sencillez, fue un algoritmo muy efectivo y se considera la base conceptual de muchos otros métodos. El cifrado de Polibio presentaba, además, una ventaja adicional al resto. Al codificar el texto en números, permitía poder comunicarlo a través de otros métodos como, por ejemplo, señales luminosas.

El texto de Polibio mostraba que la tabla está ordenada en orden alfabético. Sin embargo, si la tabla fuera ordenada de forma aleatoria y solo emisor y receptor la conocieran, se aumenta el nivel de seguridad de forma relevante. Sin embargo, este método puede ser criptoanalizado de forma sencilla mediante un simple análisis de frecuencia.

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

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

FIGURA 2: Cifradores de Polibios

Así, el cifrado de la máxima: EX ABUNDANTIA CORDIS OS LOQUITUR con el tablero de la parte izquierda viene dado por:

1553 11124533141133442411 133442142443 3443  
3134414524444542

*Ilustración 4: Cifrado de Polibio*

## Cifrado de César

Uno de los métodos más conocidos en la antigüedad es el cifrado de César. Consiste en un método de sustitución que conserva la estadística del lenguaje, donde cada letra era desplazada por la que se encontraba en el alfabeto tres posiciones hacia adelante. Si, por ejemplo, se aplicara este método en nuestro alfabeto, la letra A pasaría a ser la D, la B se sustituiría por la E y así sucesivamente (la Z es sustituida por la C en el texto cifrado).

Supone un método muy sencillo y fácil de criptoanalizar, por lo que en la actualidad ha caído en desuso. A día de hoy, se considera un cifrado de César a cualquier método que utilice el mismo método, independientemente del desplazamiento. A pesar de su sencillez, supone la base de muchos métodos de cifrados y, para aumentar la complejidad y la seguridad mejorando así los métodos

criptográficos, bastaría con no hacer siempre las mismas sustituciones, es decir, que la A no sea siempre D en el texto cifrado.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	0	1	2
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C

*Ilustración 5: cifrado de César*

## Criptoanalistas árabes

En la Edad Media, los árabes dominaban hasta siete métodos de cifrado. Gracias a sus avances y estudios sobre el criptoanálisis, publicaron el primer tratado en hablar de ello. Los árabes utilizaban la criptografía en cualquier ámbito de la vida cotidiana. Incluso los funcionarios lo utilizaban para almacenar de forma segura determinados archivos y datos. Sin embargo, los árabes no destacan por el uso criptográfico en la historia, sino por los grandes avances que tuvieron en los criptoanálisis.

Los árabes fueron capaces de criptoanalizar el método de sustitución monoalfabética, que hasta aquel momento era un método fiable, sólido y seguro. Sin embargo, aún destacan por ser los pioneros en los análisis estadísticos de la criptografía. En un inicio, el Corán se encontraba desordenado. Quisieron plasmar todas las sabidurías transmitidas por Mahoma, pero eran tantas a lo largo de los años que no se tenía constancia del momento exacto ni el orden. Los árabes se propusieron ordenar el Corán analizando la forma de hablar y de expresarse de Mahoma, ya que con el paso del tiempo las expresiones varían. Sin embargo, fueron un paso más allá y decidieron estudiar las letras de cada frase y cada capítulo, llegando a la conclusión que no todas ellas son igual de frecuentes en el lenguaje.

No se tiene constancia de quién fue el primero en aplicar este tipo de criptoanálisis, pero este estudio del Corán llevó a un punto clave en la historia de la criptografía: el análisis de la frecuencia de las letras. Al-Kindi desarrolló más la idea del análisis de frecuencias. Este estableció la idea de analizar todas las letras de una lengua para estudiar su frecuencia y clasificarlas en grupos, realizando posteriormente lo mismo con las letras del texto cifrado y sustituyendo unas por otras. Para que el proceso fuera efectivo, el tamaño del texto cifrado debe ser bastante grande, es decir, cuanto mayor es el tamaño del texto cifrado el proceso se vuelve más efectivo.



*Ilustración 6: Al-Kindi*

## Cifrado de Battista

El camino entre la sustitución monoalfabética y el cifrado de Vigenere fue bastante largo. No es hasta 1460, cuando León Battista Alberti comenzó a dar el primer paso en ese camino. Battista trabajó para tres papas y, mientras que un día estaba paseando por los jardines del Vaticano, le propusieron que cifrara los mensajes del Vaticano, a lo que aceptó de forma inmediata. Durante su estudio sobre la criptografía desde entonces, se dio cuenta de que todas las metodologías dadas hasta ese momento tenían un único problema común: el alfabeto utilizado para codificar y descodificar siempre era el mismo.

Durante una larga reflexión, llegó a la conclusión de que si se alternaban varios alfabetos durante el cifrado y descifrado, el análisis mediante frecuencias se volvía inútil y el punto débil común desaparecería. De esta forma, desarrolló el cifrado de Battista entre 1466 y 1470. El método se basa en un disco metálico (conocido como disco de Alberti). Este disco estaba formado por dos anillos, uno fijo en el centro y otro móvil rodeando al primero. Esto hace que el número de posibles cambios para una determinada letra se convierta en el tamaño del alfabeto utilizado.

Para transmitir un mensaje mediante este cifrado, el emisor y receptor deben disponer de un disco de Alberti cada uno, además de tener el mismo anillo interno con el mismo orden del alfabeto. Antes de la encriptación, el emisor debe avisar al receptor de dos letras, cada una en un anillo, que se encuentran enfrentadas. A partir de este momento, la codificación se realiza sustituyendo las letras del anillo interno por las enfrentadas en el externo, mientras que el descifrado sustituye las letras del anillo externo por las del interno.

Para evitar un ataque de frecuencias, Battista añadió la posibilidad de cambiar la posición del anillo externo en cualquier momento. Partiendo del disco que el mismo utilizaba, con un anillo interno de letras minúsculas y un anillo externo de mayúsculas, cuando en el mensaje cifrado se encontraba una mayúscula quería decir que se debe mover el anillo externo, tomando como referencia esa letra mayúscula. Este método supuso un gran avance en la historia de la criptografía y ofrecía mucha mas seguridad ante otros métodos de la época.

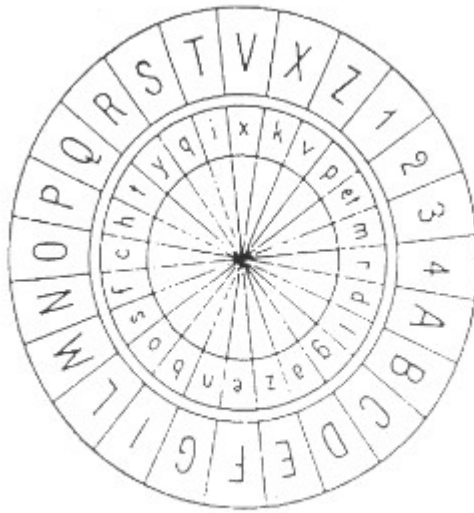


FIGURA 3. Cifrador de Leon Battista Alberti (1466)

### *Ilustración 7: Cifrado de Battista*

## Cifrado de Vigenère

Giovan Battista Bellaso, un italiano del siglo XVI, diseñó un método para la generación de claves en el uso de varios alfabetos. Bellaso propuso en 1553 seleccionar una clave y un texto en cualquier idioma, presentarlos en un papel y hacer que cada letra del texto en claro coincidiera con una letra de la clave (repetiendo esta hasta el final del texto). El proceso de cifrado consiste en sustituir la letra del texto en claro por el alfabeto que marcaba la letra de clave que le correspondía.



AB	a	b	c	d	e	f	g	h	i	l	m
	n	o	p	q	r	f	t	u	x	y	z
CD	a	b	c	d	e	f	g	h	i	l	m
	t	u	x	y	z	n	o	p	q	r	f
EF	a	b	c	d	e	f	g	h	i	l	m
	z	n	o	p	q	r	f	t	u	x	y
GH	a	b	c	d	e	f	g	h	i	l	m
	f	t	u	x	y	z	n	o	p	q	r
IL	a	b	c	d	e	f	g	h	i	l	m
	y	z	n	o	p	q	r	f	t	u	x
MN	a	b	c	d	e	f	g	h	i	l	m
	r	f	t	u	x	y	z	n	o	p	q
OP	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	f	t	u
QR	a	b	c	d	e	f	g	h	i	l	m
	q	r	f	t	u	x	y	z	n	o	p
ST	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	f	t	u	x	y	z	n	o
VX	a	b	c	d	e	f	g	h	i	l	m
	u	x	y	z	n	o	p	q	r	f	t
YZ	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	f	t	u	x	y	z	n

*Ilustración 8: cifrado de Giovan Battista Bellaso*

Giovanni Battista Della Porta fue otro pionero italiano más al cifrado polialfabético. En el siglo XVI, Battista Della Porta propuso un sistema criptográfico basado en la idea de Bellaso, en el que la clave indicaba que tipo de alfabeto había que utilizar en cada paso. Para ello, se propone una matriz con varios alfabetos donde están descritos, cada uno de ellos, en dos filas. Todos los alfabetos disponen de una de sus filas con las letras ordenadas en un orden aleatorio. De este modo, se selecciona la letra que se quiere cifrar y/o descifrar y se sustituye por la que se encuentra arriba o abajo de esta. A continuación se muestra un ejemplo:

Supongamos que queremos cifrar el texto ETPS... con la clave DOM. Lo primero que se debe hacer es ir a la matriz de alfabetos y localizar las filas pertenecientes a la letra D. Supongamos que disponemos de las dos siguientes filas

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

*Ilustración 9: filas correspondientes a la letra D en la matriz de Battista Della Porta*

El siguiente paso consiste en cifrar los dos primeros caracteres del texto plano. La letra E es sustituida por la que se encuentra en la fila inferior, V, mientras que la T se sustituye por la superior C. El siguiente par de letras en el texto debe ser cifrado con las filas correspondientes a la letra O de la matriz. Se extraen las filas y se repiten los mismos pasos hasta terminar el texto plano, mientras que la clave se repite de forma cíclica.



FIGURA 4. Cifrador de Giovanni Battista Della Porta (1593)

*Ilustración 10: Cifrador de Battista Della Porta  
(1593)*

Basándose en las ideas descritas por Bellaso, Porta y Battista, el diplomático francés Vigenère publicó el método de sustitución polialfabética más importante y conocido en la historia de la criptografía en 1585.

El cifrado de Vigenère consiste en acordar que alfabeto se va a utilizar y en que orden a través de una clave. El algoritmo de cifrado se basa en hallar la posición de las letras del texto en claro en el alfabeto y sustituirlas por la letra correspondiente a la misma posición en el alfabeto indicado por la clave. Por ejemplo, si la clave es HOLA y el mensaje LOCO, la letra L (posición 12) se encriptará como la letra de la posición 12 en el alfabeto que empieza por la letra H, la letra O se sustituirá por la letra en la misma posición en el alfabeto que empieza por O, y así sucesivamente, manteniendo una clave cíclica, hasta que se acabe el texto plano.

Este método eliminaba por completo la frecuencia, la fuerza bruta (el número de posibilidades es demasiado grande) y la probabilidad del idioma. Con el paso del tiempo se han desarrollado técnicas para criptoanalizarlo. Un primer paso para ello es conocer la longitud de clave con algunas técnicas como el test de Kasiski o los índices de coincidencia.

En estas condiciones, el cifrado *Vigenère* de: C'EST LA VIE CHER AMI con la clave PARIS es REJB DP VZM UWEI IEX, puesto que:

C	E	S	T	L	A	V	I	E	C	H	E	R	A	M	I
2	4	18	19	11	0	21	8	4	2	7	4	17	0	12	8
P	A	R	I	S	P	A	R	I	S	P	A	R	I	S	P
15	0	17	8	18	15	0	17	8	18	15	0	17	8	18	15
R	E	J	B	D	P	V	Z	M	U	W	E	I	I	E	X
17	4	9	1	3	15	21	25	12	20	22	4	8	8	4	23

Ilustración 11: ejemplo de Cifrado de Vigenère

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

Ilustración 12: Cifrado de Vigenère

## La Cifra General

En España, durante el reinado de Felipe II, se empleó el cifrado conocido como La Cifra General (1556). Este método de cifrado disponía de más de 500 símbolos y es considerada como una clave diplomática maestra. Este sistema se encuentra formado por tres partes:

1. Un vocabulario, donde cada letra se puede cambiar por un signo a escoger.
2. Un silabario, que era utilizado para cifrar grupos de dos o tres letras.

3. Un diccionario de términos comunes.

a	b	c	d	e	f	g	h	i	l	m	n
4 7 ω	∩ ^ 	∪ >	◇ <	∩ + +o	∫ g	f p	p d	g f g	∩ ∞	L θ	Γ 6
o	p	q	r	s	t	v	x	y	z		
L Le 4	∩ ∇	∩ Δ	ε ∩	ze c	z x	o ∫ a	∩ d	g Z	∩ ω		

Ilustración 13: vocabulario de La Cifra General

pa u- 61	pe u' 62	pi -u 63	po u+ 64	pu ue 65	qua r- 66	que r' 67	qui -r 68	quo r+ 69	quu re 70
pa φ- 71	pe φ' 72	pi -φ 73	po φ+ 74	pu φe 75	sa c- 76	se c' 77	si -c 78	so c+ 79	su ce 80
ta x- 81	te x' 82	ti -x 83	to x+ 84	tu xe 85	va p- 86	ve p' 87	vi -p 88	vo p+ 89	vu pe 90
xa g- 91	xe g' 92	xi -g 93	xo g+ 94	xu ge 95	ya v- 96	ye v' 97	yi -v 98	yo v+ 99	yu ve c
za c- c-	ze c' c'	zi -c -c	zo c+ c+	zu ce ce	cha g- g-	che g' g'	chi -g -g	cho g+ g+	chu ge ge
ca g- g-	ce g' g'	ci -g -g	co g+ g+	cu ge ge	fra r- r-	fre r' r'	fri -r -r	fro r+ r+	fru re re
gra ψ- ψ-	gre ψ' ψ'	gri -ψ -ψ	gro ψ+ ψ+	gu ψe ψe	pla H- H-	ple H' H'	pli -H -H	plo H+ H+	plu He He
pra D- D-	pre D' D'	pri -D -D	pro D+ D+	pu De De	tra h- h-	tre h' h'	tri -h -h	tro h+ h+	tru he he

Ilustración 14: silabario de La Cifra General

La Cifra General es muy fácil de criptoanalizar, por lo que era de esperar un rápido criptoanálisis. En febrero de 1557, el secretario del papa Triphon Bencio consiguió romperlo en apenas tres meses de uso. Bencio interceptó una carta enviada al cardenal Francisco Pacecco, usuario de la Cifra General. Con esto, Bencio consiguió descifrar una parte del texto, ofreciéndolo al público general en el libro Aloys Meister *Die Geheimschrift im Dienste der Päpstlichen Kurie von ihren Anfängen bis zum Ende des XVI.*

[1557.]

Cifra del card. di Burgos<sup>1</sup> con il re Philipppo, decifratra alli X febraro 1557  
in Bologna.

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	y	z
⚡	∩	.	L	ℓ	.	.	.	G	∞	.	Γ	ℓ	.	.	Δ	ℓ	.	a	q	
ω	Λ			+				T			6				ε	-e		ot		
			ba	be	bi	bo	bu				pa	pe	pi	po	pu					
			m	ṁ	-m	m+	mφ				u	ú	-u	u+	uφ					
											61	62	63	64	65					
			ca	ce	ci	co	cu				qua	que	qui							
			16	17	18	19	20				τ	τ̇	-τ							
			n	ṅ	-n	n+	nφ				66	67	68							
			da	de	di	do	du				ra	re	ri	ro	ru					
			21	22	23	24	25				φ-	φ̇	-φ	φ+	φφ					
			e	ė	-e	e+	eφ				71	72	73	74	75					
			fa	fe	fi	fo	fu				sa	se	si	so	su					
			a	à	-a	a+	aφ				∞	∞̇	-∞	∞+	∞φ					
											76	77	78	79	80					
			ga	ge	gi	go	gu				ta	te	ti	to	tu					
			Q	Q̇	-Q	Q+	Qφ				×	×̇	-×	×+	×φ					
			31	32	33	34	35				81	82	83	84	85					
			ha	he	hi	ho	hu				va	ve	vi	vo	vu					
			36	37	38	39	40				p-	ṗ	-p	p+	pφ					
			ia	ie	ii	io	iu				86	87	88	89	90					
			e	ė	-e	e+	eφ													
			41	42	43	44	45				xa	xe	xi	xo	xu					
			◇	◇̇	-◇	◇+	◇φ				g-	ġ	-g	g+	gφ					
											91	92	93	94	95					
			la	le	li	lo	lu				za	ze	zi	zo	zu					
			5-	5̇	-5	5+	5φ				ε	ε̇	-ε	ε+	εφ					
			46	47	48	49	50				96	97	98	99	-					
			ma	me	mi	mo	mu				gra	gre	gri	gro	gru					
			ω-	ω̇	-ω	ω+	ωφ				ψ-	ψ̇	-ψ	ψ+	ψφ					
			51	52	53	54	55													
			na	ne	ni	no	nu				cha	che	chi	cho	chu					
			o-	ȯ	-o	o+	oφ				g-	ġ	-g	g+	gφ					
			56	57	58	59	60													

Ilustración 15: parte de la Cifra que Triphon Bencio consiguió descifrar

## Cifrado de Playfair

Este método de cifrado de sustitución dinámica fue desarrollado por el inventor y científico inglés Charles Wheatstone y Lyon Playfair. Estos amigos disponen de una gran anécdota. En ocasiones, Wheatstone y Playfair se reunían para leer los mensajes criptográficos de la prensa y sacar así el texto en claro. En una ocasión, descifraron un mensaje de amor de un joven de Oxford en el periódico The Times. Ellos, por seguir el juego y utilizando el mismo método y clave para enviar el mensaje, enviaron otro mensaje que posteriormente fue respondido con “Querido Charlie, no escribas más. Nuestro cifrado ha sido descubierto”.

El cifrado de Playfair era un método sencillo y parte de una clave que debe ser acordada por el emisor y el receptor a través de un canal seguro. A continuación, se crea una matriz de 5x5, donde se escribe la clave al comienzo de la misma y posteriormente el abecedario, sin repetir palabras y juntando en la misma casilla la i y la j. Por ejemplo, si nuestra clave fuera NAPOLEÓN, la matriz quedaría de la siguiente forma:

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

*Ilustración  
16: ejemplo  
de matriz  
del cifrado  
de Playfair*

Una vez que se dispone de la matriz, se procede al algoritmo de cifrado. Para cifrar, el texto plano debe ser dividido en pares de letras que no se repitan, por ejemplo mp es correcto mientras que pp no. En los casos incorrectos, se le debe añadir una letra en el medio, pero no puede cambiar el sentido del mensaje. Si la longitud del mensaje es impar, también se le debe añadir una letra al final del texto que no modifique el sentido del lenguaje. Por ejemplo, perro se dividiría en pe-rr-o, deberíamos añadir una letra en el par rr, un ejemplo de como quedaría puede ser pe-rl-ro.

Ahora, en cada par de letras nos encontramos tres opciones de sustitución:

1. Si ambas letras se encuentran en la misma fila se sustituyen por las letras situadas a su derecha y, si alguna letra se encuentra al final de la fila, se vuelve al inicio de la misma línea.
2. Si ambas letras se encuentran en la misma columna, se sustituyen por las letras que se encuentran debajo de cada una y, si alguna letra se encuentra al final, se vuelve al inicio de la misma.
3. En otro caso, para sustituir la primera letra se debe localizar la letra situada en la misma fila que la primera letra y la columna que comparta con la segunda letra a cifrar, y para cifrar la segunda letra se debe localizar la letra situada en la misma fila que la segunda letra y la columna que comparta con la primera letra a cifrar.

El proceso de descifrado consiste en invertir el proceso. Si queremos cifrar el texto “En mis dominios nunca se oculta el sol” con este método de cifrado y la clave NAPOLEÓN, se obtiene:

Texto en claro en dígrafos: En-mi-sd-om-in-io-sn-un-ca-se-oc-ul-ta-el-so-lx.

Texto cifrado: GE GK TC LK GP KP QP QL BP QC PD ZF RO FN TP PZ

*Ilustración 17: ejemplo de cifrado de Playfair*

Este cifrado se puede criptoanalizar con un análisis de frecuencias de pares de letras. Sin embargo, los criptoanalistas de la época no disponían de técnicas para poder hacerlo vulnerable. Este método recibe el nombre de Playfair y no de Wheatstone ya que Playfair fue el promotor del método de cifrado, consiguiendo que los británicos lo adoptaran como su medio de encriptación.



*Ilustración 18: Cifrado de Playfair*

## Código Morse

En el 1837, Samuel Morse publica el código que lleva su nombre. El código morse consiste en un sistema criptográfico de representación de símbolos y letras a través de señales emitidas de forma intermitente.

Signo	Código	Signo	Código	Signo	Código
A	· —	N	— ·	0	— — — — —
B	— · · ·	Ñ	— — · — —	1	· — — — —
C	— · — ·	O	— — — —	2	· · — — —
CH	— — — —	P	· — — ·	3	· · · — —
D	— · ·	Q	— — · —	4	· · · · —
E	·	R	· — ·	5	· · · · ·
F	· · — ·	S	· · ·	6	— · · · ·
G	— — ·	T	—	7	— — · · ·
H	· · · ·	U	· · —	8	— — — · ·
I	· ·	V	· · · —	9	— — — — ·
J	· — — —	W	· — —	.	· — · · · —
K	— · —	X	— · · —	,	— · — · — —
L	· — · ·	Y	— · — —	?	· · — — · ·
M	— —	Z	— — · ·	"	· — · · — ·
				!	— — · · — —

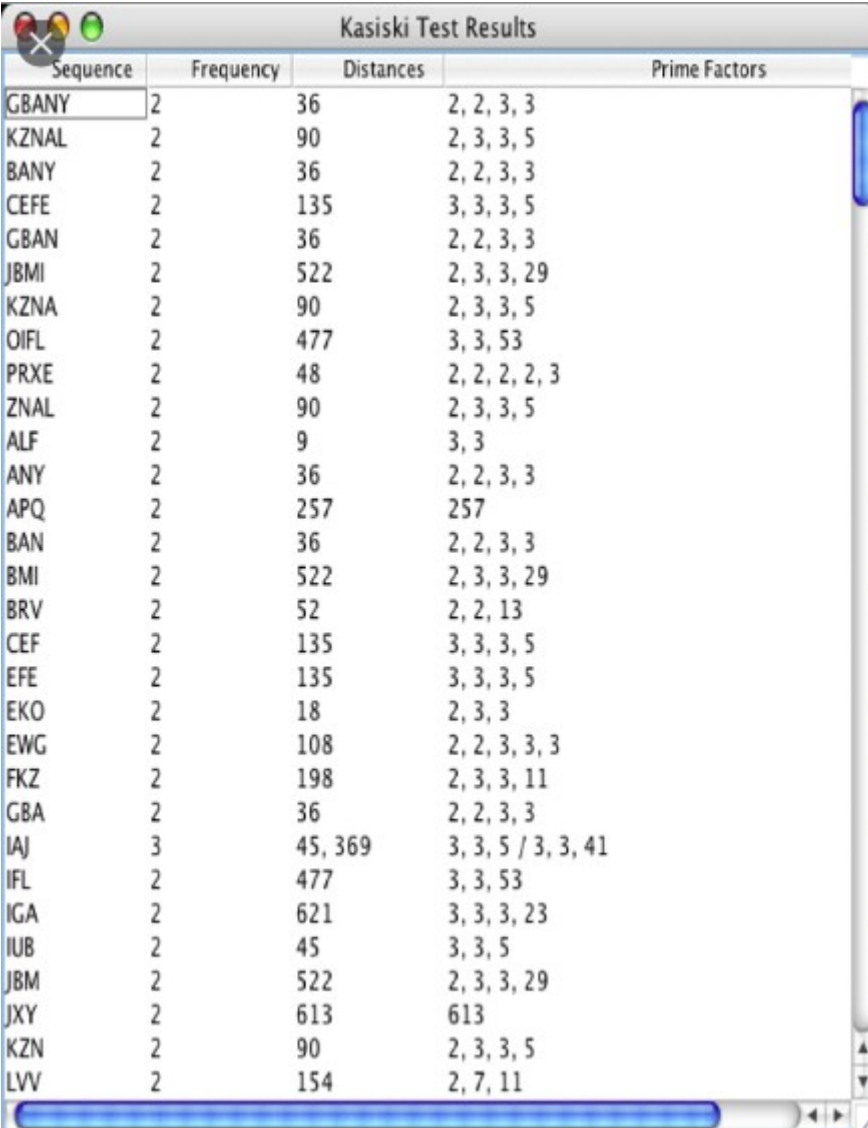
**convenciones:** — : raya (señal larga) · : punto (señal corta)

*Ilustración 19: albateto Morse*

## Kasiski y los papeles de Beale

En 1863, se publica la primera ruptura de los cifrados polialfabéticos por Kasiski. Este método de criptoanálisis es utilizado para conseguir la posible longitud de clave utilizada en los cifrados de Vigenère. Se basa en la búsqueda de repeticiones de palabras a lo largo del texto, orientándose por la idea de que dos partes iguales del texto cifrado puede corresponder a dos partes semejantes en el texto en claro cifrados con la misma parte de la clave. Una vez localizadas estas repeticiones, se debe hacer el máximo común divisor de las distancias entre ellas, ya que se sabe que estas distancias son múltiplos de la longitud de la clave. La longitud de la clave será el máximo común divisor extraído o algún factor primo del mismo.





Sequence	Frequency	Distances	Prime Factors
GBANY	2	36	2, 2, 3, 3
KZNAL	2	90	2, 3, 3, 5
BANY	2	36	2, 2, 3, 3
CEFE	2	135	3, 3, 3, 5
GBAN	2	36	2, 2, 3, 3
JBMI	2	522	2, 3, 3, 29
KZNA	2	90	2, 3, 3, 5
OIFL	2	477	3, 3, 53
PRXE	2	48	2, 2, 2, 2, 3
ZNAL	2	90	2, 3, 3, 5
ALF	2	9	3, 3
ANY	2	36	2, 2, 3, 3
APQ	2	257	257
BAN	2	36	2, 2, 3, 3
BMI	2	522	2, 3, 3, 29
BRV	2	52	2, 2, 13
CEF	2	135	3, 3, 3, 5
EFE	2	135	3, 3, 3, 5
EKO	2	18	2, 3, 3
EWG	2	108	2, 2, 3, 3, 3
FKZ	2	198	2, 3, 3, 11
GBA	2	36	2, 2, 3, 3
IAJ	3	45, 369	3, 3, 5 / 3, 3, 41
IFL	2	477	3, 3, 53
IGA	2	621	3, 3, 3, 23
IUB	2	45	3, 3, 5
JBM	2	522	2, 3, 3, 29
JXY	2	613	613
KZN	2	90	2, 3, 3, 5
LVV	2	154	2, 7, 11

*Ilustración 20: ejemplo del test de Kasiski*

En 1885 ocurre un acontecimiento histórico hasta nuestros días: el descubrimiento de los papeles de Beale. Estos papeles consisten en una serie de documentos cifrados en los que se cree que ocultan información acerca de un tesoro. En la actualidad, siguen sin ser descifrados.

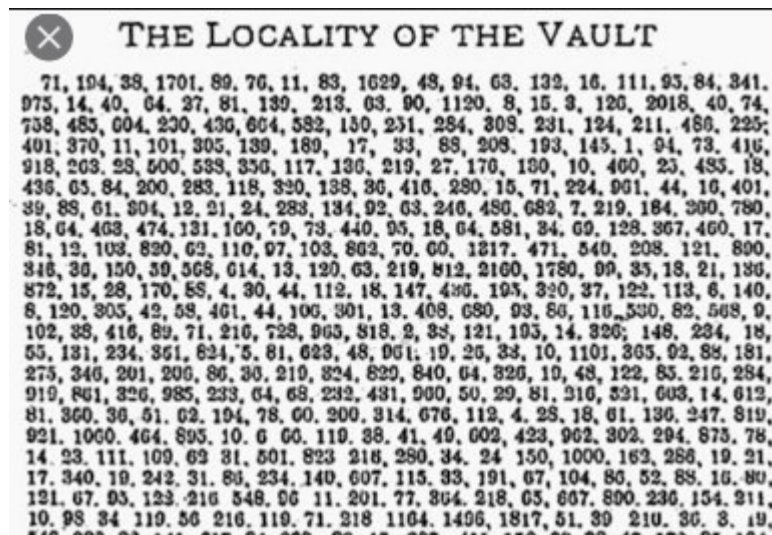


Ilustración 21: papeles de Beale

## La máquina Enigma

La máquina alemana Enigma consiste en una máquina capaz de cifrar utilizando la sustitución polialfabética, que fue usada durante la segunda Guerra Mundial. Fue creada por la empresa Scherbius y Ritter, cuyos fundadores son Arthur Scherbius (experto en motores) y Richard Ritter.

El 23 de febrero de 1918, solicitaron la patente de una máquina de cifrado basada en discos móviles que variaban su posición durante el cifrado. De esta forma, consta en la historia como la primera máquina de rotores y como la base para el desarrollo de la máquina Enigma.

En 1926 y 1928, la armada alemana encargó a la empresa Scherbius y Ritter la fabricación y adquisición de máquinas Enigma, todas ellas un poco modificadas en las versiones militares para conseguir más seguridad y avance tecnológico. Sin embargo, esta adquisición no fue rápida ni sencilla. Los alemanes tenían fuertes restricciones por los vencedores de la Primera Guerra Mundial, por lo que el precio de las máquinas rondaba los 5000 marcos (unos 20000 dólares), un coste bastante significativo que dificultó su adquisición.

Una máquina Enigma está formada de tres componentes esenciales:

1. Un teclado, en el que el emisor escribe el texto plano como si fuera una máquina de escribir.
2. El motor de cifrado. Este motor coge la letra que ha tecleado el emisor y la transforma en otra diferente. Realmente, en este motor se encuentra la esencia del cifrado, junto a sus fortalezas y debilidades. Se alimenta mediante los pulsos eléctricos generados por una batería (lo que lo hace portátil) y se caracteriza por variar el motor cada vez que se cifra una letra, generando así una pseudoaleatoriedad en el cifrado y dificultando el criptoanálisis.
3. Un panel de cifrado, donde una serie de luces le indica al emisor cual es el texto cifrado.

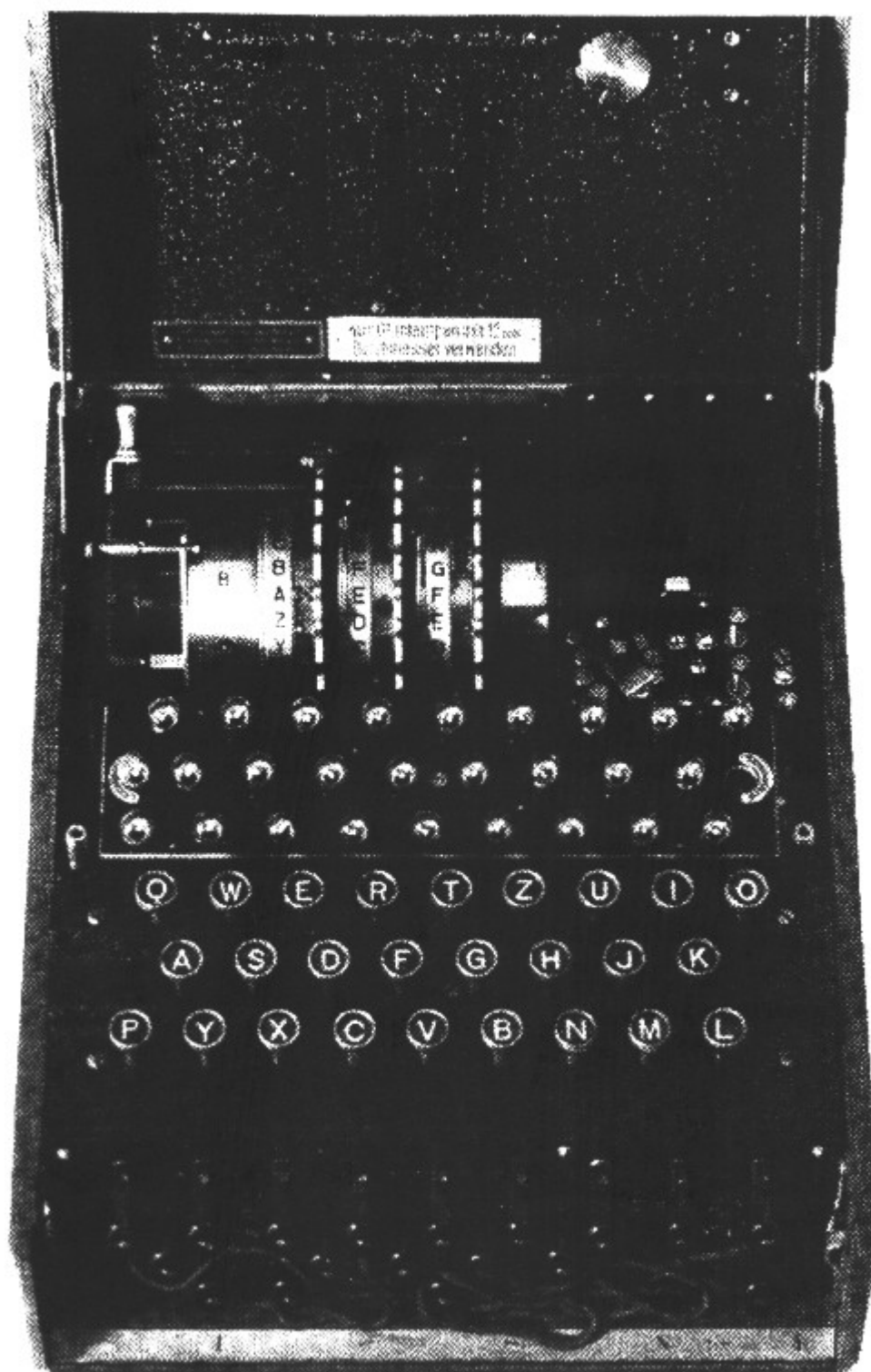


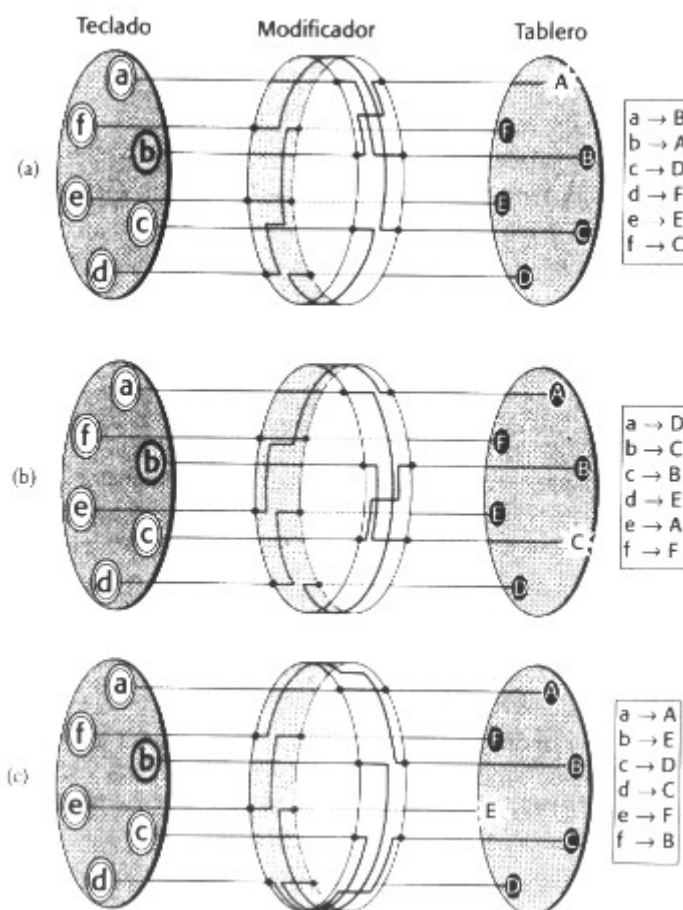
Fig. 50a. 3-rotor Wehrmacht ENIGMA (1937)

## Ilustración 22: máquina Enigma

El motor de cifrado estaba formado por un rotor, es decir, un disco con puntos metálicos y conectores eléctricos en ambas caras. Estos puntos metálicos y conectores enlazarían la entrada del

teclado con el panel de cifrado. Sin embargo, estas conexiones no son lineales, es decir, se conecta de forma irregular.

Supongamos un ejemplo sencillo del funcionamiento de la máquina Enigma, si inicialmente el rotor se encuentra en una posición donde la letra A del teclado corresponde a la D en el tablero de luces, se pulsa la letra A y el tablero de luces nos muestra la D. Sin embargo, si volvemos a pulsar la letra A no se va a iluminar la letra D, si no otra completamente aleatoria debido a que el rotor gira por cada letra encriptada.



*Ilustración 23: funcionamiento sencillo de la máquina Enigma*

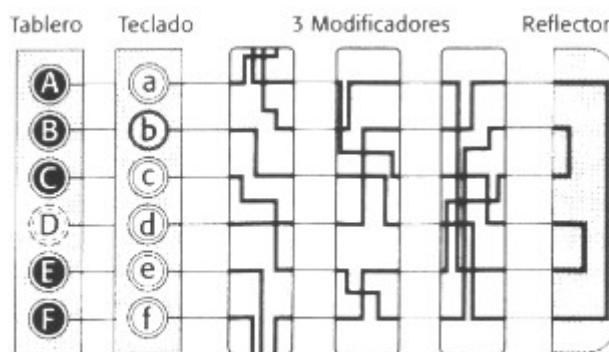
Si criptoanalizamos el sistema, podemos encontrar con la gran debilidad de la criptografía a lo largo de la historia: las repeticiones. Al estar formado por un único rotor, cuando se completa una vuelta al disco se volverán a obtener los mismos datos, es decir, en nuestro ejemplo al teclear la A nos iluminará la letra D. Por este motivo, Scherbius decidió incorporar varios rotores entrelazados. De esta forma, cuando el primer rotor completa una vuelta el segundo gira una posición y así continuamente con todos los rotores. Esto hace que el periodo de repetición se alargue.

La versión más sencilla de la máquina Enigma estaba formada por tres rotores y 26 conectores en cada cara (correspondiente a las 26 letras utilizadas). Sin embargo, las versiones más avanzadas disponían de cinco rotores diferentes con el fin de aumentar la seguridad.

A la hora de cifrar y descifrar, se debe tener en cuenta la posición inicial de los rotores, ya que una pequeña variación puede provocar un circuito muy diferente y, por lo tanto, un cifrado/descifrado diferente. El mensaje cifrado debía ser enviado en código morse y mediante radio por un operador de comunicaciones. El receptor debía escribirlo en un papel, colocar los rotores en las mismas posiciones que el emisor a la hora del cifrado y comenzar a teclear, iluminándose en el panel de cifrado las letras del texto descifrado.

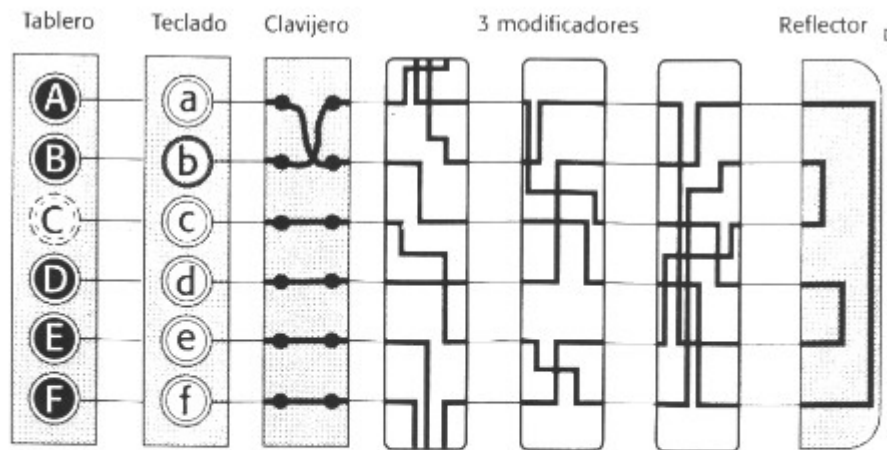
Como se ha mencionado anteriormente, las de uso militar incorporaban otras ventajas adicionales. Estas tienen añadido un tablero de conexiones de 26 clavijas (correspondientes a las 26 letras) y había 10 cables que permitían unir dos de estas letras como el emisor quisiera, de esta forma durante el circuito se sustituían unas letras por otras. Por ejemplo, si conectamos la A y la H con estos cables, al pulsar la letra A y antes de comenzar el circuito de los rotores, la letra A se sustituye por la H. De esta forma se consigue aumentar la seguridad gracias al aumento del número de configuraciones posibles.

Las máquinas militares tenían otra característica importante, el tercer rotor no se conectaba al panel de cifrado (por lo que solo tiene conectores en una cara), sino que volvía al segundo rotor y este al primero. Este tipo de rotor se conoce como reflector. El uso del reflector añadía complejidad y seguridad, pero también se generaba un punto débil, una letra en el texto plano nunca podía corresponderse con la misma letra en el texto cifrado.



**Figura 36.** El diseño de la Enigma de Scherbius incluía un tercer modificador y un reflector que devuelve la corriente a través de los modificadores. En esta posición particular, teclear la b iluminará la D en el tablero, que aquí se muestra contiguo al teclado.

*Ilustración 24: versión con reflector de la máquina Enigma*



**Figura 37.** El clavijero está colocado entre el teclado y el primer modificador. Insertando cables, es posible intercambiar pares de letras, de modo que en este caso la **b** se cambia con la **a**. Ahora, la **b** es codificada siguiendo la trayectoria que previamente se asociaba con la codificación de la **a**. En la Enigma real de 26 letras, el usuario tendría seis cables para intercambiar seis pares de letras.

*Ilustración 25: versión militar de la máquina Enigma*

## Cifrado ADFGVX

Los alemanes también introdujeron en el 1918 el cifrado ADFGVX. Este cifrado fue utilizado en la primera guerra mundial y era considerado el mejor medio de cifrado del que se disponía en la época.

Este método se divide en dos fases:

- **Sustitución:** lo primero es crear una matriz (similar a la de Polibio) en la que se introduzcan las letras y los números en el orden acordado entre el emisor y receptor. Cada columna y cada fila se encuentran identificados por un identificador. Una vez que se dispone de esta matriz, el método de cifrado consiste en intercambiar cada letra por sus coordenadas identificadas con las letras ADFGVX (texto cifrado fase 1).
- **Transposición:** con el texto cifrado anterior, se procede a realizar un nuevo cifrado. Para realizar este paso, el emisor y receptor deben acordar una palabra clave. Posteriormente, se colocan todos los caracteres del primer texto cifrado en una table encabezada por la clave establecida y se ordenan las columnas atendiendo al orden alfabético de la clave (texto cifrado fase 2).

Una vez que se han realizado ambos pasos, el mensaje final se crea copiando columna a columna, de arriba a abajo. Un ejemplo sencillo sería el mostrado en la ilustración 26.

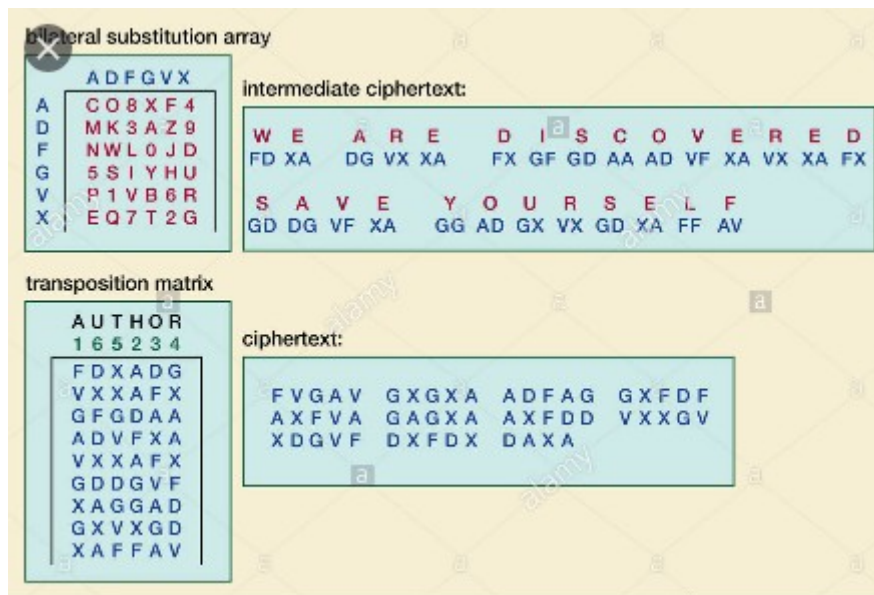


Ilustración 26: ejemplo de cifrado ADFGVX

## Principio de Kerckhoffs

En el 1474, Cicco Simonetta realiza un estudio sobre el criptoanálisis y publica sus doce puntos más críticos para realizar un buen criptoanálisis, pero no suponen las bases de los métodos actuales.

A finales del siglo XIX, el lingüista inglés Auguste Kerckhoffs estableció la base teórica para poder considerar a un criptosistema como seguro. Estas bases se denominan el principio de Kerckhoffs, y exponen que la seguridad de un criptosistema no se basa en mantener oculto en algoritmo, sino la clave. En la actualidad, todos los métodos estudiados y en desarrollo continúan aplicando dicha base.

De esta forma, en los nuevos desarrollos de métodos de cifrado, se debe tener en cuenta que un criptoanalista dispone de el algoritmo de cifrado, el algoritmo de descifrado y el mensaje cifrado. Las reglas expuestas por Kerkchoffs para asegurar que un criptosistema es seguro son las siguientes:

- “Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.”
- “La efectividad del sistema no debe depender de que su diseño permanezca en secreto.”
- “La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.”
- “El sistema debe ser operable por una única persona.”
- “El sistema debe ser fácil de utilizar.”



*Ilustración 27: Auguste Kerckhoffs*

## DES

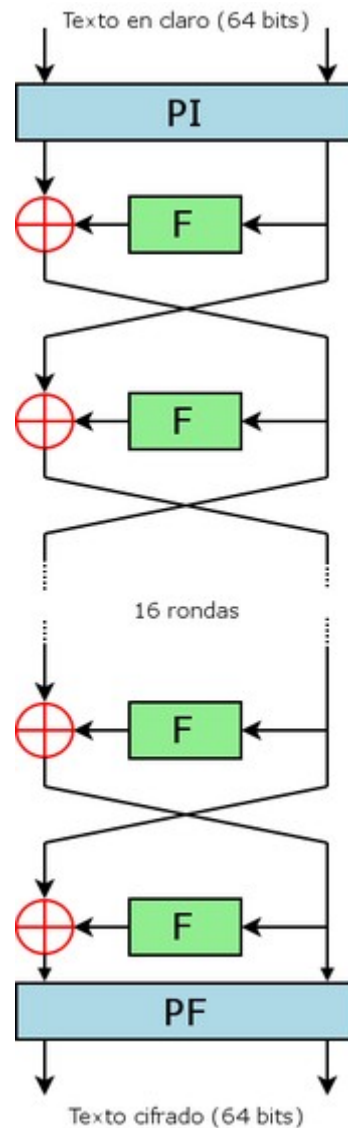
El algoritmo de cifrado simétrico Data Encryption Standard (DES) se aceptó como un estándar en 1976 por Estados Unidos, propagándose a continuación por el mundo entero. Se considera inseguro ya que el tamaño de la clave es de 56 bits (relativamente corta) y se han roto las claves del DES en menos de veinticuatro horas. A pesar de que existan posibles ataques teóricos, se considera que la variante conocida como Triple DES es segura en la práctica. Sin embargo, el algoritmo fue sustituido por el Advanced Encryption Standard (AES). En 1998, se realizó un ataque por fuerza bruta al algoritmo, demostrando así su vulnerabilidad.



Fecha	Año	Evento
15 de mayo	1973	NBS publica una primera petición para un algoritmo estándar de cifrado
27 de agosto	1974	NBS publica una segunda petición para algoritmos de cifrado
17 de marzo	1975	DES es publicado en el <i>Registro Federal</i> para comentarios
Agosto	1976	Primer taller sobre DES
Septiembre	1976	Segundo taller, sobre fundamentos matemáticos de DES
Noviembre	1976	DES es aprobado como estándar
15 de enero	1977	DES es publicado por el FIPS como estándar FIPS PUB 46
	1983	DES es confirmado por primera vez
22 de enero	1988	DES es confirmado por segunda vez como FIPS 46-1, reemplazando a FIPS PUB 46
	1992	Biham y Shamir publican el primer ataque teórico con menos complejidad que el de fuerza bruta: el <b>criptoanálisis diferencial</b> . De cualquier modo, requiere una cantidad irreal de $2^{47}$ textos planos escogidos (Biham and Shamir, 1992).
30 de diciembre	1993	DES es confirmado por tercera vez como FIPS 46-2
	1994	Se lleva a cabo el primer criptoanálisis experimental de DES utilizando <b>criptoanálisis lineal</b> (Matsui, 1994).
Julio	1998	El <b>DES cracker</b> de la EFF (Electronic Frontier Foundation) conocido como <i>Deep Crack</i> rompe una clave DES en 56 horas.
Enero	1999	De forma conjunta, <b>Deep Crack</b> y <b>distributed.net</b> rompen una clave DES en 22 horas y 15 minutos.
25 de octubre	1999	DES es confirmado por cuarta vez como FIPS 46-3, que especifica la preferencia de uso de <b>Triple DES</b> , con DES simple permitido sólo en sistemas heredados.
26 de noviembre	2001	El algoritmo <b>AES</b> (Advanced Encryption Standard) se publica como FIPS 197
26 de mayo	2002	El estándar AES se hace efectivo
26 de julio	2004	Se propone la retirada de FIPS 46-3 (y un par de estándares relacionados) en el <i>Registro Federal</i> <sup>1</sup>

*Ilustración 28: cronología de la historia del DES*

DES consiste en un algoritmo de cifrado por bloques, donde utiliza una clave, es decir, a partir de un texto de entrada con unos determinados bits fijos, lo transforma en un texto cifrado de la misma longitud aplicando diferentes operaciones intermedias y la clave de cifrado/descifrado. Emplea un tamaño de entrada, salida y clave de 64 bits. Sin embargo, el algoritmo utiliza para las operaciones intermedias 56 bits de la clave. El algoritmo es fiel a un esquema de Feistel formado por 16 rondas, una permutación inicial y una permutación final. Antes de comenzar las rondas, el texto de entrada es dividido en dos fragmentos de 32 bits cada uno.



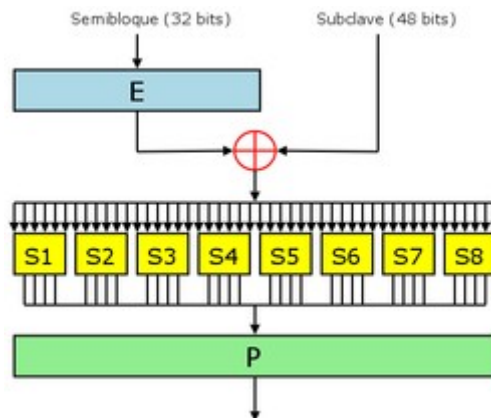
*Ilustración 29: esquema del DES*

Al utilizar el esquema de Feistel, se garantiza que el algoritmo de cifrado y descifrado sea el mismo. Únicamente se debe meter la clave en orden inverso a la hora de descifrar. La operación que aparece como + en la ilustración 29 consiste en una operación XOR, mientras que la función F mezcla la mitad de una parte del bloque con una parte de la clave.

La función F se aplica siguiendo cuatro pasos:

1. Expansión: El bloque de 32 bits es expandido a 48 bits mediante una función (E) duplicando algunos bits.
2. Mezcla: El resultado de la expansión se combina con una subclave generada de 48 bits a través de otra operación XOR.
3. Sustitución: Una vez mezclado el bloque y la subclave, el resultado debe ser dividido en ocho fragmentos de seis bits cada uno y, cada uno de ellos, debe ser reemplazado por cuatro bits atendiendo a una transformación no lineal especificada en una tabla de búsqueda denominada S-Boxes.

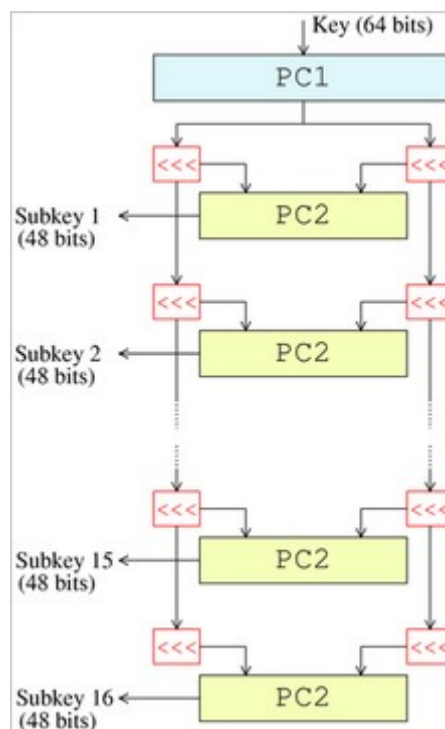
4. Permutación: Para finalizar el algoritmo, los 32 bits de salida de las S-Boxes son reordenados a través de una permutación fija.



*Ilustración 30: función F de Feistel*

El algoritmo que se sigue en la generación de subclaves es el siguiente:

1. Se escogen 56 bits de la clave mediante la primera elección permutada (PC-1). Los 8 bits restantes pueden descartarse o pueden ser comprobados como bits de paridad.
2. Se dividen los 56 bits en dos mitades de 28 bits.
3. En cada ronda, cada mitad se desplaza a la izquierda uno o dos bits (depende de cada ronda) y se selecciona la subclave de 48 bits mediante la segunda elección permutada (PC-2) como 24 bits de cada mitad.



*Ilustración 31: algoritmo de generación de subclaves*

A pesar del gran número de ataques de los que se tiene constancia para este algoritmo y los cifrados por bloques, el más práctico a día de hoy sigue siendo la fuerza bruta. Dentro de todos estos posibles ataques, cabe destacar tres de ellos que disminuyen en gran medida la complejidad ocasionada por la fuerza bruta:

- Criptoanálisis diferencial: descubierto a finales de los 80, este criptoanálisis requiere de  $2^{47}$  textos planos para poder romper el esquema de Feistel desarrollado en el DES.
- Criptoanálisis lineal: implementado por Matsui en 1994, requiere de  $2^{43}$  textos planos para romper el algoritmo.
- Ataque mejorado de Davies: este ataque fue desarrollado específicamente para el DES y requiere de  $2^{50}$  textos planos, con una capacidad funcional de  $2^{50}$  y un porcentaje de acierto de 51%.

## AES

Advanced Encryption Standard (AES) es un esquema de cifrado por bloques creado en Bélgica y desarrollado por Rijndael. El AES fue estandarizado en 2001 y desde 2006 se ha convertido en el algoritmo criptográfico simétrico más popular.

En 1997, con el fin de proteger información delicada en el siglo XXI, el Instituto Nacional de Normas y Tecnología (NIST) propuso un concurso para escoger un nuevo método de cifrado llamado Advanced Encryption Standard (AES). Los algoritmos que se presentaran al concurso deberían tener las siguientes características:

- Algoritmo público, accesible por cualquier persona.
- Cifrado simétrico con soporte de bloques con un mínimo de 128 bits.
- Claves de cifrado de 128, 192 y 256 bits.
- Implementación tanto en hardware como en software.

El concurso duró tres años y finalmente Rijndael ganó.

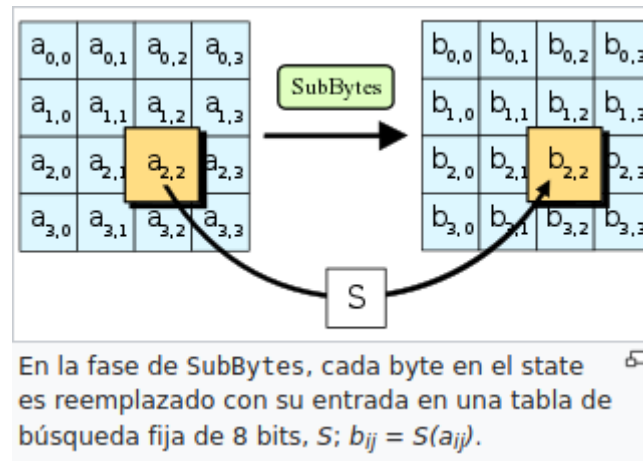
El AES consiste en una red de sustitución permutación, con una implementación sencilla tanto en hardware como en software, una gran velocidad y requiere poca memoria. El algoritmo presenta un tamaño de bloque fijo de 128 bits y un tamaño de clave de 128, 192 o 256 bits. Opera con una matriz de 4x4 llamada state y la mayoría de las operaciones realizadas a lo largo del algoritmo se hacen en un campo finito determinado. Dependiendo del tamaño de la clave, el algoritmo tiene un número variable de rondas. Si la clave tiene 128 bits aplica 10 rondas, 12 rondas para las claves de 192 bits y 14 rondas para las de 256 bits.

A continuación se muestra el pseudocódigo del algoritmo:

1. Expansión de la clave
2. AddRoundKey
3. Rondas:
  1. SubBytes
  2. ShiftRows
  3. MixColumns
  4. AddRoundKey

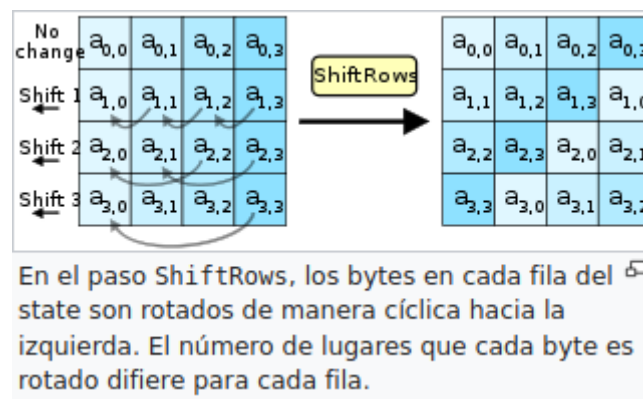
4. Final:
  1. SubBytes
  2. ShiftRows
  3. AddRoundKey

La función SubBytes se trata de una sustitución no lineal donde cada byte se reemplaza por otro atendiendo a una tabla de búsqueda.



*Ilustración 32: función SubBytes del AES*

La función ShiftRows consiste en realizar una transposición donde cada fila del state es rotada de manera cíclica un número determinado de veces.



*Ilustración 33: función ShiftRows del AES*

La función MixColumns combina los cuatro bytes de cada columna del state utilizando una transformación lineal.

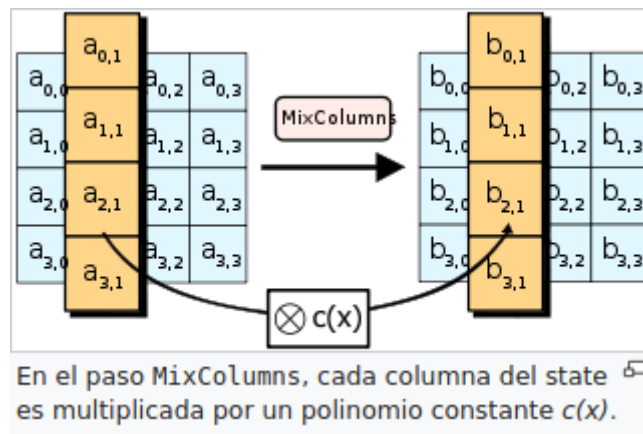


Ilustración 34: función MixColumns del AES

La función AddRoundKey combina mediante una operación XOR cada byte del state con las claves generadas a partir de una iteración de la clave.

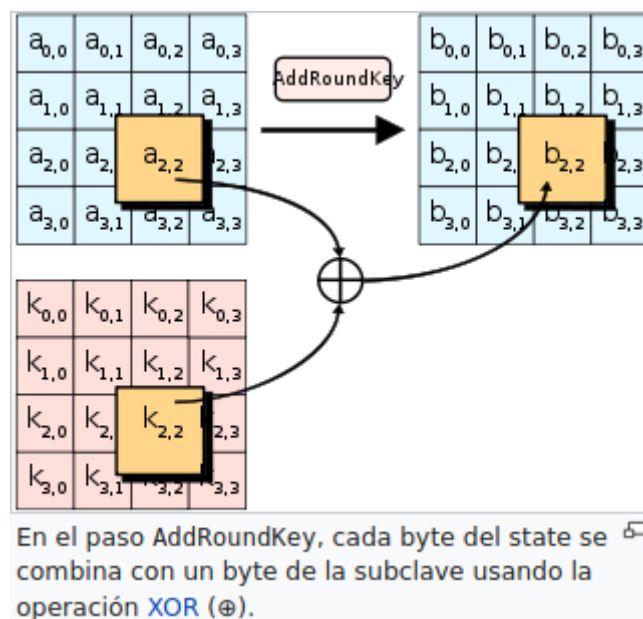


Ilustración 35: función AddRoundKey del AES

La Agencia de Seguridad Nacional de los Estados Unidos (NSA) revisó todos los algoritmos propuestos en el concurso y declaró que todos ellos eran lo suficientemente seguros como para transmitir información confidencial. En 2003, Estados Unidos anunció su seguridad y adoptó este método como el nuevo sistema de cifrado y supone la primera vez en la historia que el público tiene acceso a un sistema criptográfico destinado a la comunicación de información confidencial. Hasta 2005 no se ha registrado ningún tipo de ataque sobre este algoritmo. Estos ataques consisten en una implementación del mismo algoritmo con un número de rondas reducido, pero no han llegado a obtener el texto original. En la actualidad, el AES aún sigue siendo un método seguro ya que no se ha podido romper, pero la evolución computacional de los ordenadores y su estructura matemática lo hace vulnerable.

# Clave pública

En la década de los 70, las matemáticas fueron capaces de solucionar el gran problema de la criptografía: la distribución de claves y su creación. De esta forma, en 1976 Whitfield Diffie y Martin Hellman publicaron la propuesta de la criptografía de clave pública. Este sistema utiliza las claves, una pública para cifrar y una privada para descifrar. A este tipo de criptografía también se le denomina asimétrica debido a la separación de claves para cifrar y descifrar.

Un ejemplo sencillo de entender sería el siguiente: una persona A quiere enviar un mensaje secreto a otra B, entonces coge la clave pública de B, cifra el mensaje y se lo manda por un canal inseguro. Una vez que el mensaje llega a B, este lo descifra utilizando su clave privada. Este método destaca por su gran seguridad. Al haber cifrado A el mensaje con la clave pública de B, solamente puede ser descifrado con la clave privada de B.

El algoritmo más popular y utilizado de este tipo de criptografía es el RSA, propuesto en 1977 y cuyo nombre proviene de sus creadores, Rivest, Shamir y Adleman. Sin embargo, la NSA dificultó el desarrollo del sistema ya que lanzó acciones jurídicas contra ellos. Finalmente en 1982, crearon una empresa y pudieron desarrollar su idea por completo. A día de hoy, es un algoritmo que se utiliza a diario y está omnipresente, ya que puede ser utilizado para cifrar o firmar digitalmente.

Este algoritmo de cifrado se basa en la factorización de números enteros. Para la generación de la clave pública y privada, se siguen los siguientes pasos:

1. Se escogen dos números primos  $p$  y  $q$  distintos. Para añadir seguridad, deben ser escogidos de forma aleatoria y con un número de bits parecido. En la actualidad, estos primos son del orden  $10^{300}$ , y se encuentran en continuo crecimiento a medida que aumenta la capacidad computacional de los ordenadores.
2. Se calcula  $n$  como  $n=p*q$ .
3. Calculamos  $\phi(n)$  utilizando las propiedades de la función de Euler, en las que se establece que  $\phi(p) = p-1$  si  $p$  es primo y  $\phi(m*n) = \phi(m)*\phi(n)$  si  $m$  y  $n$  son primos entre sí. Con esto,  $\phi(n) = (p-1) * (q-1)$ .
4. Se selecciona un entero positivo  $e$  menor que  $\phi(n)$  y que sea coprimo con  $\phi(n)$ .
5. Se calcula  $d$  como  $e*d=1 \bmod \phi(n)$

Una vez aplicados los pasos establecidos, la clave pública es  $(n, e)$  y la clave privada  $(n, d)$ . El método de cifrado se realiza aplicando el cálculo  $c = m^e \bmod n$ , mientras que el método de descifrado corresponde con  $m = c^d \bmod n$ .

Aquí tenemos un ejemplo de cifrado/descifrado con RSA. Los parámetros usados aquí son pequeños y orientativos con respecto a los que maneja el algoritmo, pero podemos usar también [OpenSSL](#) para generar y examinar un par de claves reales.

$p = 61$	1º nº primo privado
$q = 53$	2º nº primo privado
$n = p \cdot q = 3233$	producto $p \times q$
$e = 17$	exponente público
$d = 2753$	exponente privado

La clave pública es  $(e, n)$ . La clave privada es  $(d, n)$ . La función de cifrado es:

$$\text{encrypt}(m) = m^e \pmod{n} = m^{17} \pmod{3233}$$

Donde  $m$  es el texto sin cifrar. La función de descifrado es:

$$\text{decrypt}(c) = c^d \pmod{n} = c^{2753} \pmod{3233}$$

Donde  $c$  es el texto cifrado. Para cifrar el valor del texto sin cifrar 123, nosotros calculamos:

$$\text{encrypt}(123) = 123^{17} \pmod{3233} = 855$$

Para descifrar el valor del texto cifrado, nosotros calculamos:

$$\text{decrypt}(855) = 855^{2753} \pmod{3233} = 123$$

*Ilustración 36: ejemplo de comunicación RSA*



# Bibliografía

- [1] <https://es.wikipedia.org>
- [2] Historia de la criptografía-Manuel J.Prieto (2020)