INTECO
Instituto Nacional de Tecnologías de la Comunicación

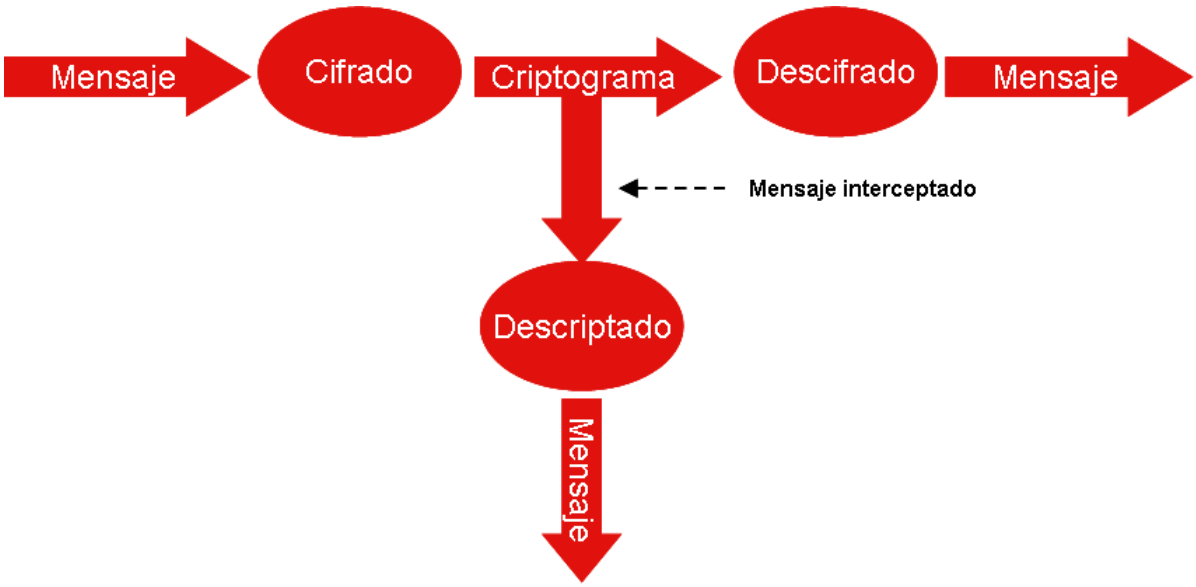
LA CRIPTOGRAFÍA DESDE LA ANTIGUA GRECIA HASTA LA MÁQUINA ENIGMA

Del griego *criptos* (oculto) y *logos* (tratado), la criptología se puede definir como la ciencia que estudia las bases teóricas y las implementaciones prácticas para garantizar la privacidad en el intercambio de información.

La criptología puede dividirse en dos partes fundamentales: la criptografía y el criptoanálisis. La criptografía se centra en las técnicas para cifrar la información, mientras que el criptoanálisis se basa en los mecanismos utilizados para descodificar dicha información, es decir, busca romper los procedimientos de cifrado y así conseguir el mensaje original.

En la Ilustración 1 se observa el canal que sigue un mensaje cuya información se quiere hacer secreta mediante técnicas criptológicas.

Ilustración 1: Canal de un mensaje secreto



Fuente: INTECO

La criptografía es una técnica muy antigua, y durante mucho tiempo se ha relacionado con los círculos militares, religiosos y comerciales. Actualmente, la necesidad de proteger la información ha hecho que la utilidad de la criptografía se haya extendido a actividades comunes. Otras aplicaciones aparte de la comunicación segura de información es la autenticación de información digital (firma digital).

.

Las técnicas criptográficas se remontan a la antigüedad, y ya en el año 400 a.C. aparecen las primeras prácticas. A continuación se enumeran algunas de ellas así como su evolución a lo largo de la historia.

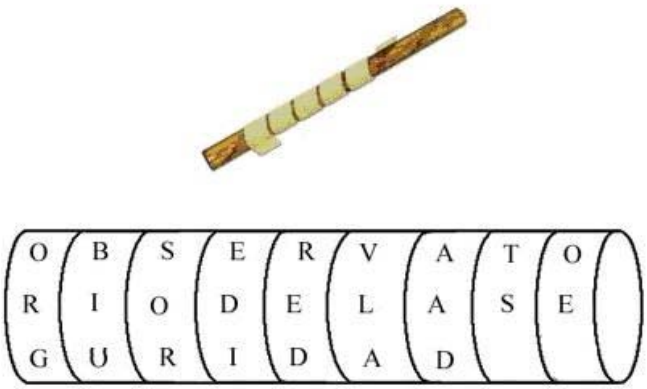
La escitala espartana

El origen de esta técnica se remonta al año 400 a. C. Era utilizada en la antigua Grecia por los espartanos para enviar mensajes ocultos entre las tropas militares.

La escitala era un listón de madera en el que se enrollaba una tira de cuero. Sobre esta tira se escribía el mensaje que se quería ocultar en columnas paralelas al eje del palo. Al desenrollar la tira se muestra un texto incoherente (aparentemente) con el texto inicial, pero que puede leerse volviendo a enrollar la tira sobre un palo del mismo diámetro que el primero.

Así, si el mensajero era interceptado, el mensaje que se encontraba era una serie de caracteres incomprensibles. Este procedimiento requiere que el emisor y el receptor del mensaje dispongan de un listón del mismo diámetro para poder descifrar el comunicado.

Ilustración 2: Escitala espartana



Fuente: INTECO

Tablero de Polibio

El historiador Polibio (nacido en el año 200 a. C.) ideó un código que se basaba en un tablero conocido como “Tablero de Polibio” (Ilustración 3) para transmitir mensajes a larga distancia. En este tablero de dimensiones 5x5 cada letra es equivalente a una pareja de ellas, correspondiendo a la fila y a la columna que forman sus coordenadas.

Ilustración 3: Talero de Polibio

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

Fuente: INTECO

Así si se quiere cifrar un mensaje se sustituye cada una de las letras que lo forman por el par de letras que le corresponden en el tablero.

INTECO ► BDCCDDAEACCD

Si en el "Tablero de Polibio" se introducen cifras en lugar de letras para formar las coordenadas de cada uno de los caracteres se consigue una variante interesante que ha servido de base para otros sistemas de cifrado.

Cifrado Cesar

Remontándose al 100 a.C. el "Cifrado Cesar" nació con la necesidad de ocultar información escrita en latín por parte del ejército de Julio César.

La técnica utilizada para cifrar un mensaje en el "Cifrado Cesar" era sustituir cada una de las letras del mensaje por aquella que ocupaba tres posiciones más en el alfabeto.

Ilustración 4: Método de Julio César

Original	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrado	d	e	f	g	h	i	j	k	l	m	n	o	p

Original	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrado	q	r	s	t	u	v	w	x	y	z	a	b	c

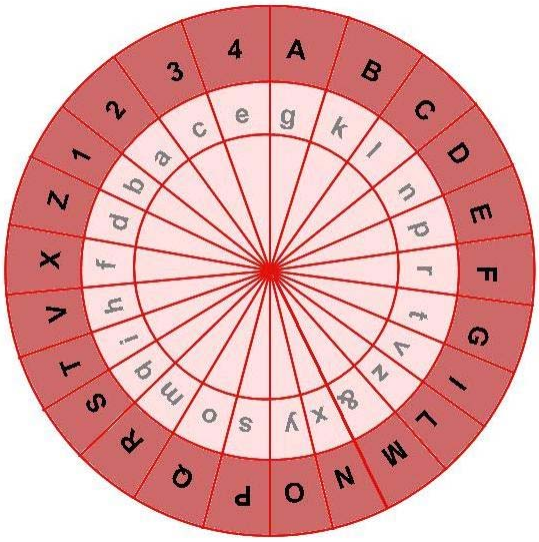
Fuente: INTECO

Disco de Alberti

Leon Battista Alberti en el siglo XV crea un disco cifrador mediante el cual es posible transformar textos sin que exista una correspondencia única entre el alfabeto del mensaje y el alfabeto usado para el cifrado. Con este sistema, cada letra del texto que se desea cifrar se corresponde con un carácter distinto dependiendo de la clave secreta utilizada.

El disco (Ilustración 5) está compuesto por dos anillos concéntricos. El externo es fijo, y contiene 24 casillas abarcando los 20 caracteres en latín (sin incluir la H J K Ñ U W Y) y los números 1, 2, 3, y 4 para el texto a cifrar. Y el interno es móvil, disponiendo de los 24 caracteres en latín además del signo & para el texto cifrado. Las 20 letras del disco externo están en orden alfabético al contrario que las 24 minúsculas del disco interno.

Ilustración 5: Disco de Alberti



Fuente: INTECO

Al ser 24 los caracteres representados en cada disco, es posible definir hasta 24 sustituciones diferentes; es decir, dependiendo de la posición que tenga el disco interior la cantidad máxima de alfabetos de cifrado es igual a 24. Luego, para cifrar un mensaje, una vez establecida la correspondencia entre caracteres de ambos discos, se convierte cada letra del texto que se desea cifrar en la letra correspondiente del disco interior.

Cifrado de Vigenère

Lo que actualmente se conoce como “Tablero de Vigenère” tiene sus orígenes en el siglo XVI. Es una generalización del cifrado anterior, ya que es una disposición de letras que contiene en orden los 26 alfabetos de César.

Adicionalmente, suele introducirse una palabra clave constituida por una palabra o texto que se repite a lo largo de todo el mensaje que se desea cifrar. Tomando la letra de la clave que se corresponde con la letra a cifrar se busca su alfabeto de César equivalente que empieza con esa letra.

Para cifrar mediante este método se procede de la siguiente manera:

1) Se busca una palabra clave sencilla que se pueda recordar fácilmente.

2) Se escribe la palabra debajo del mensaje que se quiere cifrar, repitiéndola tantas veces como sea necesario.

3) Cada letra del texto a cifrar se codifica con el alfabeto de la tabla marcado por la letra inferior (de la palabra clave) correspondiente.

En el ejemplo expuesto a continuación se puede apreciar el desarrollo a seguir para cifrar un mensaje mediante el "Cifrado de Vigenère".

Ejemplo

Texto a cifrar: Observatorio de la Seguridad

Palabra clave: MALWARE

Se escribe la palabra clave debajo del texto a cifrar como se aprecia en la Ilustración 6.

Ilustración 6: Proceso del cifrado de Vigenère

O	B	S	E	R	V	A	T	O	R	I	O	D	E	L	A	S	E	G	U	R	I	D	A	D
M	A	L	W	A	R	E	M	A	L	W	A	R	E	M	A	L	W	A	R	E	M	A	L	W

Fuente: INTECO

Una vez hecho esto cada una de las letras del mensaje se transforma en otra. Tomando la primera, la O, se observa que la que le corresponde en la palabra clave es la M. Entonces se busca en el Tablero de Vigenère el alfabeto que comienza con la letra M y la letra que le corresponde a la O, es decir, la letra A.

En la Ilustración 7 se expone el proceso para convertir la primera letra del mensaje a cifrar.

Ilustración 7: Tablero de Vigènere

0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fuente: INTECO

El mensaje cifrado utilizando la palabra clave “malware” se corresponde con:

OBSERVATORIO DE LA SEGURIDAD ► ABDARMFFOCEO UI XA DAGIVUDLZ

Cifrado de Beaufort

En el s XVIII Francis Beaufort crea un cifrado modificando el anterior (Cifrado de Vigenère), con la diferencia de que se cifra de manera inversa.

Se busca dentro de la columna de cada letra del mensaje a cifrar la letra de la clave que le corresponde y así, la letra del mensaje cifrado corresponde con la de la fila. En la Ilustración 8 se observa como se lleva a acabo el proceso (teniendo en cuenta que el texto a cifrar y la palabra clave coinciden con las del Cifrado de Vigenère en la Ilustración 6).

Ilustración 8: Tablero de Vigenère para utilizar el Cifrado de Beaufort

0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fuente: INTECO

El mensaje cifrado queda de la siguiente manera:

OBSERVATORIO DE LA SEGURIDAD ► YZTSJWETMUOM OA BA TSUXNEXLT

Cifrado Vernam

En 1917 Gilbert Vernam inventa un cifrado basado en un sistema de sustitución a través de un alfabeto binario (cinco dígitos binarios por cada carácter alfabético). Con este método se abordan cuestiones probabilísticas mediante la generación de números aleatorios.

La mayor utilización del "Cifrado Vernam" fue durante la segunda guerra mundial por espías de varios países. Durante muchos años se sostuvo la teoría de que este método era totalmente seguro, pero en 1949 se demuestra matemáticamente las técnicas necesarias para descriptar el mensaje cifrado.

Los pasos a seguir para cifrar un mensaje son:

- Transformamos el mensaje original a código binario.

- Se crea la clave a través de una secuencia binaria aleatoria de la misma longitud que el texto que se desea cifrar.
- Se suma el mensaje original y la clave mediante una suma módulo 2[1] y la operación resultante es el mensaje cifrado.

Mediante el siguiente ejemplo se ilustran los pasos seguidos para cifrar el mensaje.

Ejemplo	
Texto a cifrar: **INTECO**	
Texto a cifrar en código binario:	01001 01110 10100 00101 00011 01111
Clave aleatoria en código binario:	00011 11111 10101 10010 01110 10111
Suma módulo 2 (texto cifrado):	01010 10001 00001 10011 01101 11000

Con lo que el texto original se convierte en:

INTECO ► 01001 01110 10100 00101 00011 01111

La cifra ADFGVX

En 1918 los alemanes introdujeron este sistema de cifrado antes de lanzar su ofensiva sobre la ciudad de Paris.

Para este método de cifrado se dibuja una cuadrícula de 7x7 y se rellena la primera fila y la primera columna con las letras A, D, F, G, V y X. Los 36 cuadrados interiores se completan de manera aleatoria con las letras del alfabeto y los 10 dígitos.

El procedimiento de disposición de la cuadrícula forma parte de la clave, con lo que debe ser conocida por el receptor para poder descifrar los mensajes.

Una vez que se dispone del tablero (Ilustración 9) la primera fase para cifrar el mensaje original es localizar cada una de las letras que lo forman en dicho tablero y sustituirlas por el par de letras que corresponden a su línea y a su columna, por ejemplo la “y” se convertiría en AF.

Esta primera fase no supone ninguna innovación con respecto a los métodos expuestos anteriormente.

[1] Explicando el proceso matemático de manera sencilla se puede entender que la suma módulo 2 da cómo posibles resultados 0 ó 1. Si la suma aritmética es igual a 2 ó 0 el resultado es 0 y si la suma aritmética es igual a 1 entonces la suma módulo 2 es igual a 1.

Ilustración 9: Fase 1 de la "Cifra ADFGVX"

	A	D	F	G	V	X
A	d	9	y	n	o	u
D	7	a	2	8	p	v
F	b	g	h	w	f	r
G	x	0	t	3	j	1
V	4	e	m	c	q	l
X	s	i	k	5	z	6

Fuente: INTECO

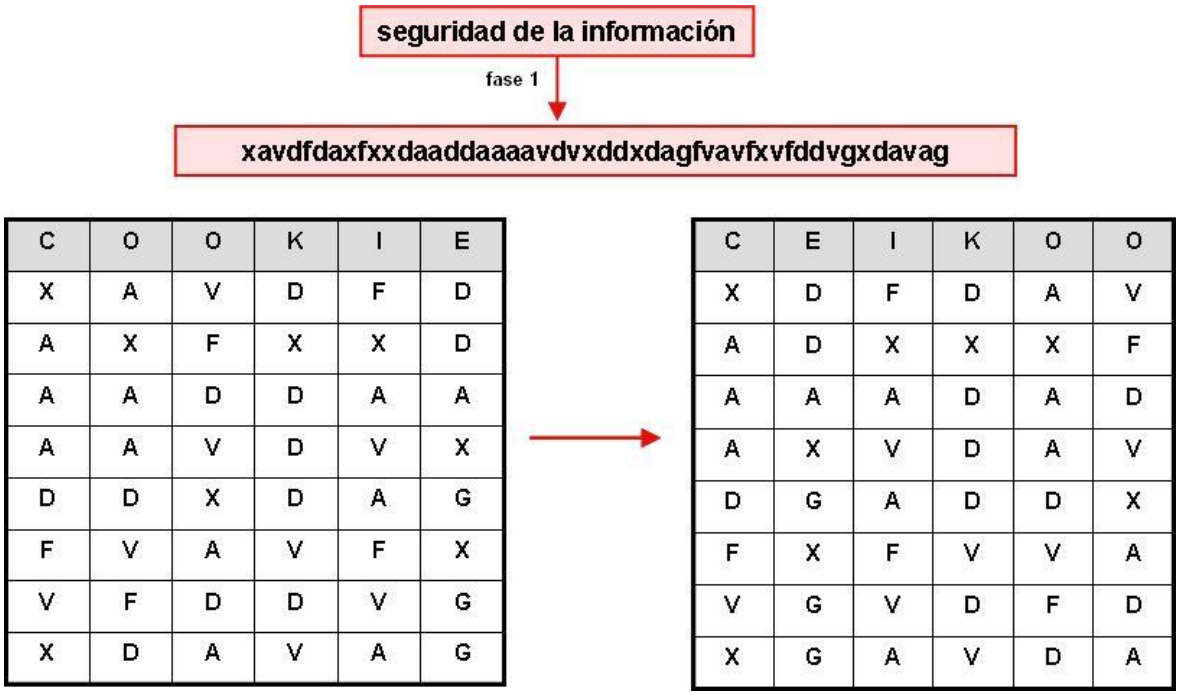
En la segunda fase del proceso de cifrado se necesita una palabra clave compartida con el receptor del mensaje procediendo de la siguiente manera:

- Las letras de la palabra clave se escriben en la fila de una nueva cuadrícula.
- Debajo de éstas se escribe el texto cifrado de la fase 1.
- Después, las columnas se cambian de posición colocándolas en el orden alfabético de la palabra clave.
- El texto cifrado se obtiene tomando este nuevo tablero por columnas y escribiendo el mensaje en este orden.
- El texto cifrado final se envía en código morse al receptor final.

El motivo de que se elijan las letras ADFGVX no es aleatorio, se basa en que estos caracteres son muy diferentes entre si cuando se convierten en las líneas y los puntos del código morse.

En la Ilustración 10 se muestra como se va a llevar a cabo el cifrado del texto teniendo en cuenta que el texto a cifrar es "seguridad de la información" y la palabra clave utilizada en este caso es "COOKIE".

Ilustración 10: Fase 2 de la "Cifra ADFGVX"



Fuente: INTECO

El texto cifrado antes y después de ser convertido en código morse quedaría:

seguridad de la información ► xaaadfvxddaxgxggfxavafvadxdddvdvaxaadvfdvfdvxada

-..- .- .- .- -.. ..-. ...- -..- -.. -.. .- -..- --. -..- --. --. ..-. -..- .- ...- .- ..-. ...- .- -.. -..- -.. -.. -.. ...- -.. ...-

.- -..- .- .- -.. ...- ..-. -.. ...- ..-. -.. ...- -..- .- -.. .-

La máquina enigma

En 1918 el inventor alemán Arthur Scherbius y Richard Ritter querían sustituir los inadecuados sistemas de criptografía empleados en la Primera Guerra Mundial recurriendo a la tecnología en vez de utilizar lápiz y papel. De esta manera desarrollaron la máquina Enigma.

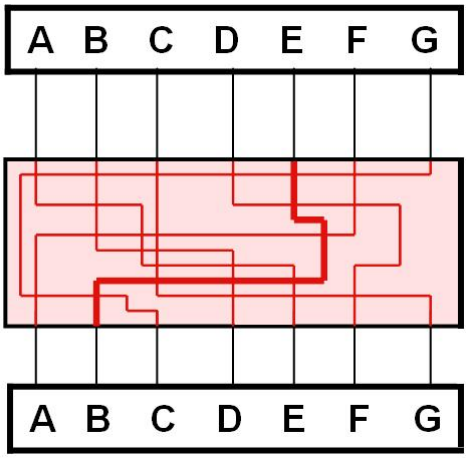
La máquina Enigma en sus inicios se componía de tres partes fundamentales: un teclado en el cual se escribía el texto que se quería cifrar, una unidad modificadora y un tablero en el que se mostraba el mensaje codificado.

En la Ilustración 11 se visualiza el proceso de cifrado de la máquina Enigma con un ejemplo en el que se han utilizado 7 letras.

Cada letra del texto a cifrar se pulsaba en el teclado y la unidad modificadora lo transformaba en otra diferente antes de mostrarla en el tablero. Así, la letra E se intercambiaba por la letra B.

Arthur Scherbius la creó de manera que cada vez que se pulsara una letra la unidad modificadora girase un veintiseisavo de vuelta (para un alfabeto completo de 26 letras), con lo que la codificación de la siguiente letra sería diferente a la de la primera.

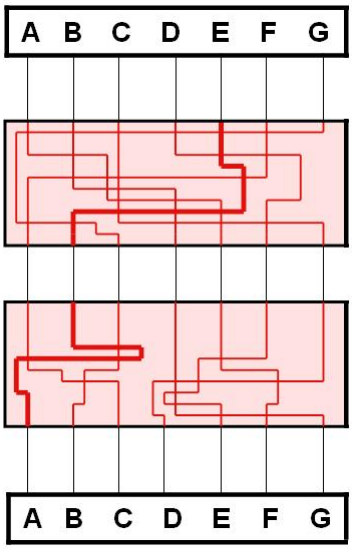
Ilustración 11: Cifrado de la máquina Enigma con un disco modificador (con 7 letras)



Fuente: INTECO

El principal problema que presentaba era que de esta forma se disponía de un cifrado de Vigenére de 26 letras el cual era fácil de descifrar. Para solventarlo Scherbius colocó una segunda unidad modificadora, de tal forma que cuando el primer disco daba una vuelta completa, el segundo giraba una posición.

Ilustración 12: Cifrado de la máquina Enigma con dos discos modificadores (con 7 letras)



Fuente: INTECO

Insertando este nuevo disco modificador se consigue pasar de una clave de 26 posiciones a una de 26*26, es decir, de 676. Mas tarde, aún se añadió otro disco más, que avanzaba una posición cuando el segundo había dado una vuelta completa consiguiendo así 26*26*26= 17.576 posiciones.

La máquina Enigma disponía de otro complemento más, el Reflector, mediante el cual, los receptores del mensaje podían descifrarlo. Cuando éste llegaba al destino los receptores estaban preparados con otra máquina Enigma con los rotores colocados en la misma posición que la máquina que enviaba el mensaje cifrado y a través del Reflector introduciendo el mensaje cifrado se reproducía el mensaje original.

Finalmente, se le añadieron dos características más:

- Los rotores eran intercambiables, de manera que como hay 6 modos de poner los tres rotores, el número de claves aumenta.
- Se introdujo un clavijero con el que se podía intercambiar pares de letras en grupos de 6.

De esta manera la máquina Enigma ofrecía billones de posibilidades de creación de claves.

El ejército alemán aseguraba que era el sistema de cifrado más seguro del mundo para sus comunicaciones, y adquirieron una gran cantidad de máquinas Enigma durante la Segunda Guerra Mundial.

Ilustración 13: Máquina Enigma

Fuente: INTECO

Los alemanes utilizaban una nueva clave cada día, para que los enemigos dispusieran de sólo 24 horas para poder descifrarla con lo que supuso el método criptográfico mas seguro hasta el momento.