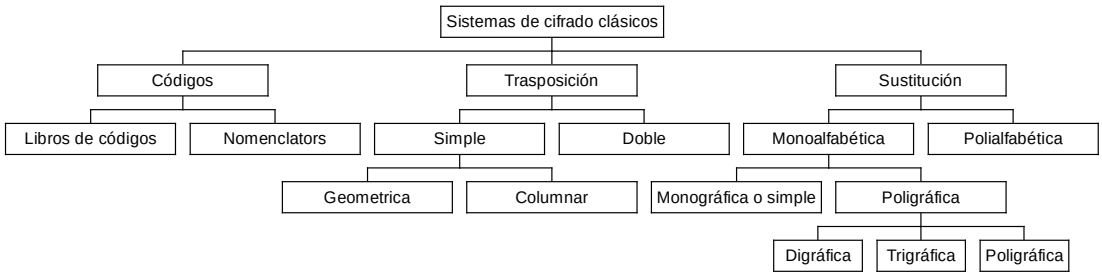
Una introducción a la Criptografía Clásica.

José Ramón Soler Fuensanta

Introducción.

La criptografía, al igual que cualquier rama del conocimiento humano, tiene su propia nomenclatura. Consideramos que es necesario conocer ésta para una mejor comprensión del tema en cuestión. Sin embargo, una mera presentación de los términos puede ser no solo aburrida, sino contraproducente. Optamos pues en presentar en este apartado los diferentes métodos, su funcionamiento, y la nomenclatura utilizada en una forma gradual y lo más práctica posible ciñéndonos al campo de la criptografía clásica. Evidentemente no están todos los métodos conocidos, pero sí alguno de los más representativos. Una introducción más profunda y más matemática puede encontrarse en cualquier libro de los muchos que hay en el mercado dedicados al estudio de la criptografía y sus métodos.



Cifrado de la información.

El cifrado de la información o *criptografía* es la ciencia que estudia el diseño de métodos para ocultar el significado de un mensaje, siendo éste públicamente disponible. Es decir se oculta el contenido del mismo pero no el mensaje. El caso contrario es el de la *esteganografía*, en ella se pretende ocultar el mensaje; una vez descubierto éste, el contenido del mismo es legible. Las formas de ocultar el contenido de un mensaje varían y las estudiaremos a continuación, por el momento nos basta con saber que el mensaje será alterado de forma que teóricamente nadie, exceptuando el legítimo destinatario, podrá leer su contenido.

Al mensaje a cifrar se le suele denominar *texto en claro* y al proceso de ocultar el contenido mediante una serie de transformaciones regidas por un parámetro o valor secreto, la *clave*, se le denomina *cifrar* el mensaje, al parámetro se le y al mensaje cifrado se le suele denominar un *texto cifrado* o un *criptograma*. Al proceso de obtener el texto en claro a partir de un mensaje cifrado se le denomina *descifrar* el mensaje. En este punto tendríamos que hablar de obtención del mensaje en claro por métodos lícitos, es decir, lo que hemos denominado como *descifrado* del mensaje, que será siempre realizado por las personas que comparten el secreto del cifrado y descifrado del mensaje, en contraposición con la obtención del significado de dicho mensaje por métodos ya no tan lícitos, es decir, la *descriptación* o el *criptoanálisis* del mensaje. No hace falta indicar que en este último caso el criptoanalista no conoce el método o la clave de descifrado.

En muchos casos el mensaje se cifra en bloques de longitud fija, a los métodos que realizan el cifrado siguiendo este esquema se les denomina cifradores en bloque, en contraposición a los cifradores de flujo, que generalmente cifran la información símbolo a símbolo, en general bit a bit. Una cosa muy corriente en los cifradores en bloque es que el mensaje no sea de un tamaño múltiplo de la longitud del bloque. En este caso se añaden al mensaje, generalmente al final del último bloque y con la intención de rellenarlo, una serie de caracteres sin valor ni significado denominados *nulos*. No es la única aplicación de los nulos, en

muchos casos se insertan en medio del texto en claro, con la pretensión de hacer más difícil la labor al posible criptoanalista.

Libros de códigos.

Este método fue ampliamente utilizado durante siglos, y aún sigue utilizándose. Consiste básicamente en la asociación de palabras o frases a palabras o grupos de letras, es decir, se trata de un tipo de sustitución muy especializado. Un texto codificado puede a su vez ser cifrado, a esto se le denomina un *supercifrado*. Como ventaja tiene el hecho de que al no existir ningún tipo de relación en el código dificulta mucho la labor del criptoanalista. Como desventaja presenta el hecho de tener que manejar un libro de códigos, en general voluminoso, lo que hace que sea fácil cometer errores. Además, no es fácil de modificar el código si este cae en manos de un potencial intruso. Hoy en día se siguen utilizando en combinación con un método criptográfico potente.

En [ROD86], [SGA90] y [GAL95] pueden verse varios ejemplos de códigos utilizados en la historia. Los libros de códigos tienen además la particularidad de que no solo sirven para ofrecer seguridad sino también economía en la transmisión, por lo cual fueron y son ampliamente utilizados tanto comercial como militarmente.

Existe asimismo una diferenciación entre los códigos en función del número de elementos que contengan. Un código con pocos elementos, hasta unos mil, se suele denominar un repertorio. El código propiamente dicho suele tener entre unos mil y unos diez mil. A un código con más de diez mil elementos, se le suele denominar un diccionario.

Nomenclátor.

El principal problema de los libros de códigos es su inflexibilidad. La inclusión de cualquier término obliga a una reescritura del mismo. Una solución para este problema es la utilización de un código mixto en el que se codifiquen ciertas palabras y se utilice el cifrado en el resto del texto. Este esquema se denomina un *nomenclátor* y, desafortunadamente, no proporciona mucha más seguridad que el libro de códigos. Una vez conocido el método de cifrado, las palabras codificadas son fácilmente deducibles por el contexto en el que se encuentran. Uno de los nomencladores más famosos fue el utilizado en la correspondencia entre Maria Estuardo y Babington, cuyo descriptado por Thomas Phelippes, secretario de cifras de Lord Walsingham, les acarreó a ambos la muerte.

Códigos de trinchera.

Inicialmente desarrollados por los franceses a partir de 1916, se denominan así a los códigos utilizados por los soldados en el frente para transmisiones durante acciones militares. Su característica principal es que son códigos reducidos, y en general orientados al uso potencial de los mismos, artillería, infantería, etc. Para aumentar su dificultad de interceptación y descifrado por el enemigo, en algunos casos se cifraban. En guerras más dinámicas, su uso por las fuerzas en combate queda descartado, ya que es muy difícil tanto la distribución como la protección de los códigos, sin embargo, la primera guerra mundial se caracterizó por ser una guerra de trincheras y fortificaciones. La estabilidad de las líneas permitió su adopción y propició su éxito. Dada su utilidad, fueron rápidamente adoptados por otras naciones, entre las cuales destacan, por su complejidad y completitud los códigos desarrollados por los alemanes. Estos constaban de hasta cuatro mil términos y eran cambiados regularmente cada dos meses.

Bustrófedon.{PRIVATE }

Se trata de la forma en la que leían y escribían los etruscos y los griegos. Esta palabra quiere decir " el buey que da vueltas" y significaba que se empezaba a leer de derecha a izquierda cambiando el sentido de la lectura en cada nueva línea.

Acróstico.

Se trata de obtener información oculta en el mismo mensaje. Básicamente consiste en utilizar la primera letra o palabra de cada párrafo o verso.

Métodos de sustitución monoalfabética.

En estos métodos se sustituye cada carácter del mensaje original por uno o varios caracteres del alfabeto utilizado como cifra. En el caso de que cada carácter se sustituya por otro se denominan métodos de sustitución monoalfabética monoliteral, siendo denominados multiliterales en el caso de que cada carácter se sustituya por un grupo de caracteres. En los métodos multiliterales el grupo de caracteres de sustitución siempre es el mismo, en caso contrario estaríamos hablando de homófonos.

Método de Julio Cesar.

Se trata de un método de cifrado monoalfabetico por sustitución atribuido a Julio Cesar. Este método lo describe Suetonio de la siguiente manera:

> Para los negocios secretos utilizaba una manera de cifra que hacia el sentido ininteligible, estando ordenadas las letras de manera que no podía formarse ninguna palabra; para descifrarlas, tiene que cambiarse el orden de las letras tomando la cuarta por la primera, esto es d por a, y así las demás."

Se trata pues del desplazamiento de tres posiciones a la derecha de las letras del alfabeto, con lo que el alfabeto quedaría como en la tabla siguiente.

Original	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
Cifrado	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

Octavio Augusto, siempre según Suetonio, utilizaría un método de cifrado similar al de Cesar, pero desplazando una sola posición el texto, "*Cuando escribía en cifra ponía la b por la a, c por b y así con las otras letras; por x ponía dos a"*.

Método de desplazamiento.

Se denominan de esta manera todos aquellos métodos que impliquen la sustitución de un carácter del alfabeto por otro desplazado *x* posiciones. Evidentemente se trata de una generalización del método de Julio Cesar en el cual la clave puede ser cualquiera en un rango entre 1 y $n - 1$, siendo n el número de elementos del alfabeto. El número de desplazamientos es la clave.

$C_k = m + k (\mathrm{mod}\, n)$ En el caso de $k = 3$ obtenemos el método de Cesar.

Este método es muy fácil de romper con la simple aplicación de técnicas estadísticas, una tabla de las posibles permutaciones o un estudio exhaustivo de las claves hasta encontrar la correcta, ya que solo hay n posibles.

Cifrado afín.

Se trata de una generalización del anterior en el que se utiliza una transformación lineal del tipo $C_k = am_k + b (\mathrm{mod}\, n)$. Tomando $a = 1$ tenemos el método de desplazamiento.

En este caso es necesario que *a* sea un entero primo con *n*, en caso contrario el descifrado podría dar lugar a ambigüedades. Sean $\left.\begin{array}{l} C_1 = am_1 + b(\mathrm{mod}\, n) \\ C_2 = am_2 + b(\mathrm{mod}\, n) \end{array}\right\}$, supongamos que $C_1 = C_2$.En este caso tenemos que $a(m_1 - m_2) = 0(\mathrm{mod}\, n)$, o lo que es lo mismo $a(m_1 - m_2) = kn$ .Con lo que para que la solución sea única y $m_1 = m_2$ debe cumplirse que *a* y *n* no tengan ningún factor común.

Sustitución por alfabetos independientes.

En este caso se generan dos alfabetos totalmente independientes haciéndose la sustitución de los caracteres cuyas posiciones coincidan. Aunque el número de posibles permutaciones es muy elevado, el criptoanálisis de este método, al igual que el de todos los de sustitución monoalfabética, es muy sencillo basándonos en las propiedades estadísticas del lenguaje.

Uno de los problemas que presenta este método es la dificultad de memorizar los alfabetos. Existe sin embargo una forma sencilla de generar un alfabetos de sustitución sin la necesidad de memorizar las equivalencias entre los mismos. Para ello basta con utilizar una palabra como clave. El alfabeto se genera poniendo la palabra clave al principio eliminando las letras duplicadas y poniendo a continuación el resto del alfabeto normal en un orden prefijado. Por ejemplo si utilizamos la palabra seguridad como clave, el alfabeto generado sería:

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

Una variante más segura de este método es el de distribuir los caracteres del alfabeto en forma de tabla y coger los datos en columnas bien en orden posicional o en orden alfabético.

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

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

Sistema bífido.

Se dice de cualquier criptosistema en el que el carácter a cifrar da como resultado una combinación de dos caracteres. Se llama trífido en el caso de que la combinación sea de tres. Equivalentemente un digrama o un trigrama es la aparición en un texto cifrado de una serie de dos o tres letras.

Cifrado de Polibio.

El historiador griego Polibio (203-120 a.c.), creó un sistema de enviar mensajes por medio de antorchas encendidas. El método consistía básicamente en la creación de una matriz cuadrada de 5 x 5 tal como la siguiente.

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

El mensaje se representaba por los números que formaban la fila y columna cuya intersección daba como resultado la letra que se quería enviar. Si bien el método de Polibio no tenía inicialmente un propósito criptográfico, sí que es la base de sistemas posteriores y el primer caso conocido de sustitución monoalfabética multiliteral.

Una variante del cifrado de Polibio, utilizado por los comunistas en la guerra civil española [NEW98] consistía en generar una tabla con tres filas de diez columnas. La primera fila no tenía numeración y la segunda y tercera filas se numeraban respectivamente con dos de los números no utilizados en las columnas de la primera fila. Las columnas se numeraban con una permutación de los dígitos del cero al nueve .

El proceso de cifrado consistía en poner una palabra de ocho o menos letras diferentes en la primera fila. En esta palabra se eliminaban las letras repetidas y el resto, hasta completar el alfabeto, se disponían en las dos filas siguientes. El cifrado es similar al de Polibio, pero aquí las letras pueden codificarse como uno o dos números.

Por ejemplo si tenemos el mensaje "*Atacar al amanecer*", la clave *fusil* y las columnas generadas por el siguiente orden:

	8	**3**	**0**	**2**	**4**	**6**	**1**	**7**	**5**	**9**
	F	U	S	I	L					
5	A	B	C	D	E	G	H	J	K	M
1	N/Ñ	O	P	Q	R	T	V	X	Y	Z

El mensaje cifrado sería 581658505814584585958185450541 4. El descifrado es sencillo, ya que si el dígito inicial es un cinco o un uno sabemos que es el carácter viene representado por dos dígitos, en caso contrario, por uno solo.

Sustitución homofónica.

El principal problema de los métodos de substitución monoalfabéticos es el mantener las propiedades estadísticas del alfabeto original. Para eliminar este problema existen dos soluciones, la utilización de alfabetos homófonos y la utilización de sistemas de sustitución polialfabeticos. La utilización de alfabetos homófonos tiene el inconveniente de ampliar el tamaño del mensaje, característica no deseable, pero tiene la ventaja de eliminar las frecuencias características del lenguaje original, y en algunos casos como la utilización de determinadas tablas de homófonos, la posibilidad de tener una entropía máxima del mensaje.

Básicamente una sustitución homofónica es una correspondencia de uno a muchos en lugar de una correspondencia uno a uno típica de los métodos de sustitución monoalfabéticos. Se asigna a cada letra del alfabeto original un conjunto de elementos de un alfabeto ampliado o de elementos agrupados de un alfabeto. Los subconjuntos que se asignan a cada una de las letras del alfabeto original deben ser evidentemente disjuntos.

Por ejemplo una asignación podría ser la siguiente.

Texto en claro	Homófonos
A	01,05,23,12,17
B	18,03,56
C	22,25,02
D	09,27
E	06,26,87,54,36

Las tablas de homófonos pueden utilizarse secuencialmente o bien aleatoriamente. Es decir, en el primer caso, la primera aparición de la letra en claro A daría como resultado el 01 como cifra, la segunda aparición el 05 y así sucesivamente hasta la finalización del conjunto de homófonos para esa letra, punto a partir del cual se empezaría el proceso otra vez con el 01. En este caso se habla de cifrado homofónico secuencial. En el caso de escoger aleatoriamente cualquier homófono se habla de cifrado homofónico aleatorio.

Un tipo de sustitución homofónica muy interesante es la formada por las tablas de homófonos. En este caso el alfabeto se representa por una tabla de homófonos que serán los que formaran el mensaje cifrado, siendo la clave la tabla igual que en el caso anterior y la dirección de cifrado (horizontal o vertical). Con estas tablas se puede conseguir una entropía máxima del contenido del mensaje. Para ello se coge la frase a cifrar y una frase cuyo significado sea el contrario, se escriben una encima de la otra y se utiliza una para las filas y otra para las columnas. El cifrado será la intersección de ambas letras. La entropía es máxima en este caso pues si el descifrado se realiza verticalmente dará un resultado, y si se hace horizontalmente dará el contrario. Si no se conoce la dirección de cifrado, es imposible estar seguro de cual es el mensaje real.

Sea por ejemplo la matriz siguiente:

	T	O	D	N	A
T	012	015	023	056	152
O	142	136	825	651	874
D	354	625	177	853	444
N	123	145	156	167	198
A	199	299	399	499	599

```
Mensaje       :TODO
Mensaje falso :NADA

Filas    T   O   D   O
Columnas N   A   D   A
Cifrado 056 874 177 874
```

En el caso hipotético de que el criptoanalista obtuviese la tabla, no podría estar seguro del mensaje, ya que si se escogen las columnas el mensaje da por resultado NADA y si se escogen las filas el resultado es TODO. Solo podría obtenerse la solución correcta en el caso de que se supiese con certeza cual es la dirección de cifrado.

Métodos de sustitución polialfabética.

En todos los cifrados anteriores se utilizaba un solo alfabeto para cifrar, lo que permitía el análisis del cifrado por métodos estadísticos al conservar el texto cifrado las características básicas del alfabeto original. De hecho el método del análisis de frecuencias se conocía desde el siglo IX, en el que fue descrita por Abú Yusuf Yaqub ibn Ishaq ibn as Sabbah ibn ´omran ibn Ismail al Kindi.

Un método para evitar este problema es utilizar varios alfabetos de forma que se disimulen las características del lenguaje fuente. Esta es la base de los sistemas denominados polialfabéticos.

Cifrado de Alberti.

Leon Battista Alberti (1404-1472) fue un criptógrafo florentino considerado por muchos como el padre de la criptografía occidental. Fue el prototipo de hombre del renacimiento

interesado en múltiples campos del saber y la cultura. Escribió tratados de arquitectura, poesía y diseñó la famosa Fontana de Trevi y el palacio Pitti. Su principal aportación en el campo de la criptografía es su disco de cifrado, el primer uso conocido de cifrado polialfabético, y el primer texto escrito de criptoanálisis, unas 25 páginas escritas en 1466, en las que estudia las frecuencias de aparición de las letras en latín e italiano y como estos aspectos pueden ayudar a resolver criptogramas.

El disco de Alberti está formado por dos discos concéntricos que giran independientemente. En el disco exterior, aparecen 20 letras ordenadas alfabéticamente y los números del 1 al 4. En el disco interior aparecen las letras del alfabeto latino desordenadas. El disco externo se utiliza para el texto en claro y el interno para el texto cifrado. El cifrado es sencillo se escogen una letra del alfabeto cifrado y una del alfabeto en claro que formarán la clave. Se sitúan los dos círculos de forma que las letra escogidas como clave coincidan. A partir de ese momento se sustituyen las letras del mensaje por las del alfabeto cifrado que coincidan en la posición donde aparece la letra en claro. El descifrado es la operación inversa.

Alberti recomendaba que cada cierto número de palabras se desplazasen los discos, obteniéndose de esta manera un cifrado polialfabético.

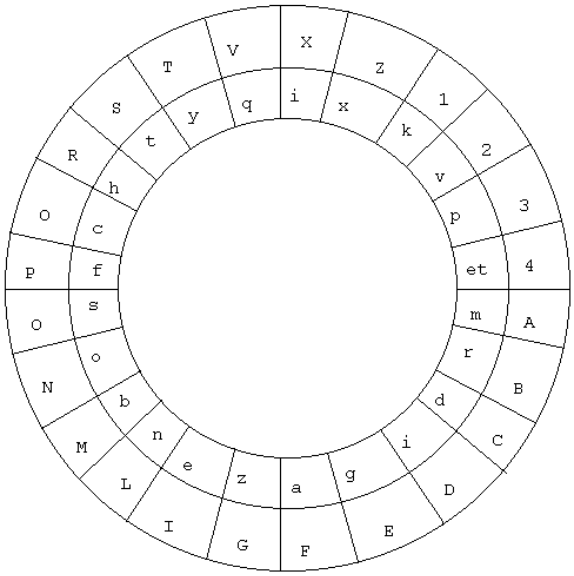


Tabla de Porta.

Giovanni Battista Porta (1535-1615), al igual que Alberti, fue el típico prototipo de hombre del Renacimiento. Nacido en Nápoles, en su primer libro *Magia Naturalis* hacía un análisis detallado de la magia y como podía utilizarse para controlar el entorno. En el libro también se describían toda una serie de técnicas esteganográficas. Fue sin embargo el *De Furtivis Literarum Notis* el que le encumbró en la historia de la criptografía. En este libro presenta una clasificación de los métodos conocidos en su época y un método digráfico conocido con su nombre.

La tabla de Porta está formada por una matriz como la siguiente:

AB	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
CD	a	b	c	d	e	f	g	h	i	j	k	l	m
	z	n	o	p	q	r	s	t	u	v	w	x	y
EF	a	b	c	d	e	f	g	h	i	j	k	l	m
	y	z	n	o	p	q	r	s	t	u	v	w	x
GH	a	b	c	d	e	f	g	h	i	j	k	l	m
	x	y	z	n	o	p	q	r	s	t	u	v	w
IJ	a	b	c	d	e	f	g	h	i	j	k	l	m
	w	x	y	z	n	o	p	q	r	s	t	u	v
KL	a	b	c	d	e	f	g	h	i	j	k	l	m
	v	w	x	y	z	n	o	p	q	r	s	t	u
MN	a	b	c	d	e	f	g	h	i	j	k	l	m
	u	v	w	x	y	z	n	o	p	q	r	s	t
OP	a	b	c	d	e	f	g	h	i	j	k	l	m
	t	u	v	w	x	y	z	n	o	p	q	r	s
QR	a	b	c	d	e	f	g	h	i	j	k	l	m
	s	t	u	v	w	x	y	z	n	o	p	q	r
ST	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
UV	a	b	c	d	e	f	g	h	i	j	k	l	m
	q	r	s	t	u	v	w	x	y	z	n	o	p
WX	a	b	c	d	e	f	g	h	i	j	k	l	m
	p	q	r	s	t	u	v	w	x	y	z	n	o
YZ	a	b	c	d	e	f	g	h	i	j	k	l	m
	o	p	q	r	s	t	u	v	w	x	y	z	n

Para cifrar con este método se escribe el mensaje en una línea y la clave en la línea anterior encima del mensaje, repetida tantas veces como sea necesario para que contemple todo el mensaje. El siguiente paso es la aplicación de la tabla para el cifrado, para ello se escoge la letra de la fila superior y se busca su equivalente en la parte izquierda de la tabla. Una vez seleccionadas las filas, se busca la letra del mensaje en ambas, sustituyendo el carácter por el de la otra fila.

El proceso de descifrado es idéntico al de cifrado simplemente sustituyendo el texto en claro por el texto cifrado.

Por ejemplo, si queremos cifrar la palabra ALBERTI con la clave PORTA, tendríamos:

```
Palabra clave : PORTAPO
Texto en claro: ALBERTI
Texto cifrado : TRTVEAO
```

Método de Vigenère.

El diplomático francés Blaise de Vigenère en su obra de 1586 *Traité des chiffres ou secrètes manières d'écrire* propone la utilización de una tabla cuadrada de alfabetos regulares. Este método fue utilizado durante siglos en los ejércitos de diferentes países, entre otros por el ejercito confederado en la guerra de secesión en Estados Unidos, considerándose indescifrable hasta la aparición del libro de Kasiski en 1863. Sin embargo, se ha seguido utilizando, con pequeñas variaciones, hasta hace relativamente pocos años, entre otros por el ejercito español que lo denominaba *cifrado con el cuadro tipo S-51*.

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

En el cifrado con esta técnica se utiliza una tabla similar a la anterior en la que están definidos los 26 alfabetos posibles con un desplazamiento unitario en cada fila.

Básicamente la formula que rige el cifrado viene dada por la siguiente formula:

$$c_i = E_{k_i}(m_i) = (m_i + k_i) \bmod n$$

siendo la clave $K = k_1, k_2, .., k_p$ el conjunto formado por todos los desplazamientos de los caracteres de la clave con respecto al alfabeto básico. El descifrado viene dado por la formula:

$$m_i = D_{k_i}(c_i) = (c_i - k_i) \bmod n$$

El cifrado y descifrado utilizando la tabla es muy sencillo. Primeramente se sitúa el mensaje en una línea y la clave repetida tantas veces como sea necesario en la línea siguiente, a la altura del mensaje original y empezando por la misma posición. El carácter cifrado vendrá dado por la intersección de los caracteres del mensaje en claro y la clave. El descifrado se realiza de la misma manera únicamente variando la utilización del mensaje cifrado en lugar del original, y de la columna de clave de descifrado en lugar de la de cifrado.

Por ejemplo, si queremos cifrar la frase CIFRA INDESCIFRABLE con la clave Vigenère tendríamos:

V	I	G	E	N	E	R	E	V	I	G	E	N	E	R	E	V	I	
C	I	F	R	A	I	N	D	E	S	C	I	F	R	A	B	L	E	
X	Q	L	V	N	M	E	H	Z	A	I	M	S	V	R	F	G	M	

Cifrado de Beaufort.

Este método, una variante del de Vigenere, fue en realidad un invento de Jean Sestri en 1710 [SAC51], pero es vulgarmente conocido con el nombre del almirante inglés Sir Francis Beaufort. Básicamente la formula que rige el cifrado viene dada por la siguiente formula:

$$c_i = E_{k_i}(m_i) = (k_i - m_i) \bmod n$$

siendo la clave $K = k_1, k_2, ., k_p$ el conjunto formado por todos los desplazamientos de los caracteres de la clave con respecto al alfabeto básico. El descifrado viene dado por la formula:

$$m_i = D_{k_i}(c_i) = (k_i - c_i) \bmod n$$

Para realizar el proceso de cifrado se procede a preparar el par (mensaje, clave) como en el caso anterior, el cifrado se realiza buscando la letra del mensaje en claro en la fila superior. Posteriormente se busca en la columna que apunta esa letra la correspondiente a la clave. El carácter cifrado es el identificador de la fila encontrada. Por ejemplo la letra C con la clave J se cifrará en la tabla anterior con la letra H.

Autoclave.

En realidad no se trata de un método de cifrado en sí, sino de una utilización particular de la clave de cifrado. El método de cifrado puede ser cualquiera, aunque generalmente se utiliza el de Vigenère en la que el texto en claro o el propio cifrado se utiliza como clave. Originalmente desarrollada por Girolamo Cardano sobre 1550, fue mejorada por Blaise De Vigenère. Se trata únicamente de aumentar el tamaño de la clave. Inicialmente se parte de una palabra clave y a continuación se utiliza el texto en claro o el cifrado producido hasta entonces como clave.

Por ejemplo si utilizamos la frase CLAVE DE CIFRADO MUY LARGA tal como lo utilizaba Cardano tendríamos:

Clave: CLAVE CL CLAVEDE CLA CLAVE
Texto: CLAVE DE CIFRADO MUY LARGA

Utilizando la mejora al método descrita por Vigenère tendríamos:

Clave: RCLAV ED ECIFRAD OMU YLARG
Texto: CLAVE DE CIFRADO MUY LARGA

Métodos de sustitución poligráfica.

Al contrario que los métodos anteriores en los cuales un carácter del texto en claro era sustituido por su equivalente cifrado, en los métodos de sustitución poligráfica se sustituyen grupos de caracteres en claro por sus equivalentes cifrados, hablándose de sustitución digráfica cuando se sustituyen pares de caracteres. El método más conocido de sustitución digráfica es el cifrado de Playfair y el de sustitución poligráfica en general el de Hill.

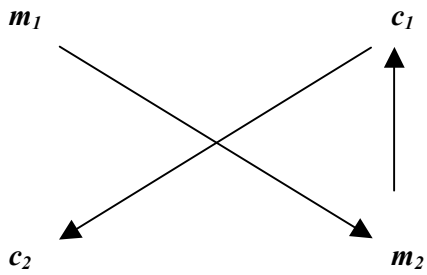
Cifrado Playfair.

Este método de cifrado fue desarrollado por Sir Charles Wheatstone alrededor del año 1854 y popularizado por su amigo Lyon Playfair, barón de Saint Andrews. Fue este último quien presentó el método al ministerio de asuntos exteriores británico que estaba buscando un método de cifrado para utilizarlo en la guerra contra los Boers. Al principio de la guerra el ejercito británico utilizaba libros de códigos, pero al ser destruidos o capturados gran parte de ellos, los oficiales empezaron a enviarse los mensajes en latín. Sin embargo, no todos los oficiales sabían latín y existía la posibilidad de que los boers tuvieran entre sus filas gente ilustrada que también conociera el latín.

Este método, con algunas variaciones, fue utilizado hasta la segunda guerra mundial debido principalmente a su sencillez y a su fácil adaptación a cualquier entorno. Se trata de un cifrado digráfico formado por una matriz cuadrada de 5x5 elementos en los que se introducen las letras del alfabeto, utilizándose la misma celda para la I y la J. El método de cifrado es muy sencillo. En primer lugar se colocan las letras correspondientes a la palabra que se va a utilizar

como clave, sin que haya repeticiones, y posteriormente se colocan el resto de las letras del alfabeto hasta rellenar la matriz. Una vez confeccionada la matriz de cifrado se divide el texto a cifrar en grupos de dos letras consecutivas comprobando que no existe ningún par de letras iguales. En el caso de que esto ocurra, se inserta un nulo, es decir, una letra al azar que no de lugar a confusión en el contenido del mensaje. Una vez hecho esto las reglas a seguir para cifrar son:

1) Si las dos letras a cifrar están en diagonal, el par cifrado será el formado por las letras que forman la diagonal de los otros dos vértices del rectángulo. Si el par del mensaje es m_1, m_2 y el del cifrado correspondiente es c_1, c_2 el proceso de cifrado se vería de la siguiente manera.



2) Si las dos letras a cifrar están en la misma línea horizontal, el par cifrado está formado por las letras a la derecha de ambas, siendo la primera columna la que sigue a la última y la última la que antecede a la primera. Matemáticamente podemos decir que en el caso de que la letra cifrada corresponde a la letra en claro que está en la columna de la primera más o menos uno módulo 5.
3) Si las dos letras a cifrar están en la misma línea vertical, el par cifrado está formado por las letras debajo de ambas, siendo la primera fila la que sigue a la última y la última la que antecede a la primera. Matemáticamente podemos decir que en el caso de que la letra cifrada corresponde a la letra en claro que está en la fila de la primera más o menos uno módulo 5.

El proceso de descifrado es simplemente la realización de los pasos anteriores en sentido inverso.

Una variante de este método conocido como NI por el ejercito americano era utilizado por el ejercito alemán en la segunda guerra mundial con el nombre de Doppelkastenschlussel [DAV96]. Básicamente consistía en poner dos tablas juntas tipo playfair con alfabetos distintos y hacer el cruce sobre las dos, es decir, de los dos caracteres a cifrar solo uno debía aparecer en cada tabla. Posteriormente se volvía a cifrar el resultado con el mismo método. Los alemanes cambiaban las tablas cada tres horas, con lo que el criptoanálisis era extremadamente difícil y solo al final de la guerra cuando se relajaron las normas por parte del ejercito alemán los americanos pudieron descifrar los mensajes con éxito.

Cifrado de Hill.

Lester Hill (1891-1961) era un profesor de matemáticas que entró en la historia de la criptografía por un artículo aparecido en 1929 en *The American Mathematical Monthly* con el título "Cryptography in an algebraic alphabet". En este artículo Hill proponía por primera vez la utilización de ecuaciones en aritmética modular para cifrado de información. En 1931 en otro artículo proponía la utilización de matrices para el cifrado de información. Este método de sustitución poligráfica parte de la utilización de una matriz cuadrada invertible K que se utiliza como clave. El proceso de cifrado y descifrado es como sigue:

CIFRADO

1) Codificar el mensaje en claro en forma numérica.
2) Dividir el mensaje en trozos de longitud l, siendo l el rango de la matriz *K*.
3) Realizar con los trozos del mensaje la operación $C = M.K$, siendo *C* el vector que contiene el texto cifrado y *M* el mensaje en claro.

DESCIFRADO

1) Dividir el mensaje cifrado en trozos de longitud l.
2) Calcular K^{-1}.
3) Hacer la operación $K^{-1}.C = K^{-1}.K.M = I.M = M$.

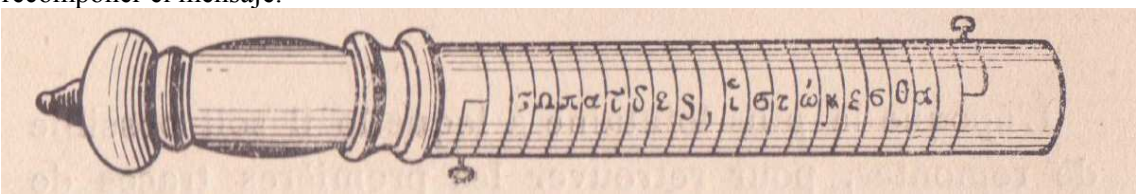
En realidad el método de Hill no es excesivamente práctico, ya que las operaciones con matrices son lentas y además obligan en el caso de no utilizar dispositivos electrónicos a guardar la clave *K* en un medio físico. Sin embargo, es la primera aproximación seria de las matemáticas a la criptografía y quizás la primera vez que se utilizaba un problema matemático, fuera de los clásicos de la permutación de elementos, como medio para cifrar información.

Métodos de transposición.

Los métodos de transposición, al contrario que los de sustitución, no pretenden llegar a obtener una distribución estadística plana. Su distribución estadística coincide plenamente con la del alfabeto de origen, sin embargo, el mensaje es inteligible al haberse realizado con los símbolos del mismo un reajuste modificando su situación en el texto. Hasta la aparición de los dispositivos de cifrado automáticos los métodos de sustitución eran preferidos a los de transposición debido a una característica no muy recomendable de estos últimos, el acarreo de errores a lo largo del documento cifrado.

Escítala lacedemonia.

Se trata del primer caso conocido de un método de transposición. Fue descrita por Plutarco como método para cifrar la información utilizado por los espartanos en el siglo V antes de Cristo. Consistía en un bastón de un determinado grosor que era utilizado por los eforos (gobernantes) para transmitir información a los estrategas (generales) durante las campañas militares y que hoy en día se considera el antecesor del bastón de mando. Para cifrar la información se enrollaba una tira de pergamino sobre el bastón y posteriormente se escribía el mensaje a lo largo del mismo de forma que cuando el pergamino se desenrollaba las letras del mensaje cambiaban de posición y si no se disponía de un bastón del mismo grosor no se podía recomponer el mensaje.



Transposición en zig-zag (rail fences).

Consiste en dividir el mensaje en varias filas de caracteres e ir cogiendo las filas consecutivamente. Matemáticamente, si *n* es el número de caracteres del mensaje, *F* el número de filas en las que se divide el mensaje, *f* el número de la fila y *p* la posición del próximo carácter a escoger, tenemos que $p = f + i\left[\frac{n}{F}\right]$ con $i = \left\{0,..,\left[\frac{n}{F}\right]\right\}$ y $p \le n$.

Por ejemplo, si queremos cifrar la frase rail fences con tres líneas, disponemos cada una de las letras en una de las líneas consecutivamente. Cuando todas están dispuestas en su posición se coge el mensaje línea a línea.

R L N S
A F C
I E E

El mensaje cifrado sería: RLNSAFCIEE.

Transposición por columnas.

En este método de transposición se escribe el mensaje en columnas debajo de la palabra clave y a continuación se escogen las columnas por orden posicional o alfabético, tal como habíamos visto al generar alfabetos de sustitución. En el caso de que queden celdas sin ocupar, se rellenan con caracteres nulos que no puedan entorpecer la lectura correcta del mensaje original Si bien es un método sencillo, fue utilizado hasta la II guerra mundial.

K	**A**	**I**	**R**	**O**
H	E	S	I	D
O	C	A	P	T
U	R	A	D	O
E	S	P	E	R
O	P	O	D	E
R	E	S	C	A
P	A	R	K	O
C	H	X	X	X

Cifra: ECRSPEAHHOUEORPCSAAPOSRXDTOREAOXIPDEDCKX[1]

Métodos de rejilla.

Los métodos de rejilla fueron utilizados desde muy antiguo como método estagenográfico. Simplemente se escribía un texto cualquiera y en determinadas posiciones se escribían las letras o palabras que tenían interés. Estas posiciones quedaban delimitadas por unos agujeros en un trozo de papel que se superponía en el texto y dejaba ver el mensaje oculto. Si no se disponía de una rejilla idéntica a la del emisor no se podía leer el mensaje. Este método ya fue descrito por Girolamo Cardano sobre 1550.

Una variación de las rejillas aparecida en el siglo XVIII son las denominadas rejillas rotativas. En estas el número total de aperturas de la rejilla es un cuarto del total de posiciones de la rejilla. La escritura del mensaje se realiza girando sucesivamente la rejilla 90º y rellenando las aperturas hasta volver a la posición original. Para hacer una rejilla con la propiedad de que al rotar no coincidan dos casillas de mensaje, basta ir fila a fila escogiendo una serie de posiciones que no hayan sido previamente marcadas y marcar con una x o cualquier otro símbolo las posiciones que ocupará al hacer las rotaciones.

[1] Mensaje enviado al ABWERH en 1941 por su agente de origen judío en Palestina Paul Fackenheim. El mensaje original era “Bin erwischt. Hoffe weg zu kommen.Koch”.[TIM96]

Métodos combinados.

La utilización de ambos métodos tanto el de sustitución como el de transposición, ha sido constante a través de la historia, el siguiente paso era la utilización de ambos métodos combinados. La combinación de las operaciones de transposición y de sustitución es la base de la mayoría de los métodos modernos de cifrado de clave secreta. El método más famoso, y quizás el primero que utiliza ambos sistemas conjuntamente para formar un sistema más potente el ADFGVX que explicamos a continuación.

ADFGVX.

El sistema ADFGVX fue desarrollado por el entonces teniente de la Reichswehr Fritz Nebel [LAS98]. Toma su nombre de la utilización exclusiva de estas letras en el texto cifrado. Este sistema, uno de los más completos y difíciles de la Primera Guerra Mundial, fue roto por George Painvin a principios de Junio de 1918 dando a los franceses la información necesaria para repeler el ataque alemán en el Somme, no conociéndose un método general de resolución hasta su publicación por Friedman en 1933.

El sistema parte de una tabla de cifrado similar a la de Polibio, de seis filas por seis columnas, en las cuales se disponen aleatoriamente 26 letras y 10 dígitos. Esta disposición cambiaba frecuentemente y podemos decir que era la clave del sistema de sustitución. El primer paso del proceso de cifrado era el mismo que el utilizado en la tabla de Polibio. Sin embargo, una vez realizado éste, se realizaba una transposición del texto cifrado. Esta, se hacía en base a una clave compartida entre los comunicantes. El orden alfabético de las letras de la clave, indicaba el orden por el que debían tomarse los caracteres en las columnas. Una vez realizado este proceso, el resultado se enviaba en Morse.

La utilización de las letras ADFGVX no es casual, estas letras son muy diferentes entre sí cuando se codifica en morse, lo que evita muchos errores en la transmisión [SIN00].

Mensaje en claro : GUERRA DE 1914

	A	**D**	**F**	**G**	**V**	**X**
A	5	Z	A	Q	6	W
D	S	1	X	E	D	9
F	C	R	F	V	7	T
G	G	B	2	Y	H	N
V	0	U	J	M	3	I
X	K	L	4	P	O	8

Cifrado sustitución: GAVDDGFDFDAFDVDGDDDXDDXF
Clave transposición: VERDUN

6	**2**	**4**	**1**	**5**	**3**
V	**E**	**R**	**D**	**U**	**N**
G	A	V	D	D	G
F	D	F	D	A	F
D	V	D	G	D	D
D	X	D	D	X	F

Cifrado final : DDGDADVXGFDFVFDDDADXGFDD

Dispositivos de cifrado.

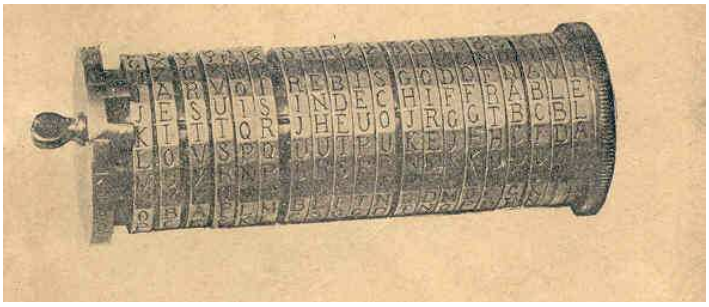
El proceso de cifrar y descifrar la información llega a un punto en el cual es inviable manualmente. El aumento de seguridad de los sistemas obliga a realizar más pasos y a que estos sean más complejos lo que conlleva mayor riesgo de cometer errores si estos procesos se hacen en entornos en los que la velocidad sea un requerimiento. Llegados a este punto la solución más obvia para eliminar los problemas mencionados, es sin duda la mecanización. Si bien los discos de Alberti se pueden considerar un precursor de los dispositivos de cifrado, es en los siglos XIX y fundamentalmente en la primera mitad del siglo XX, hasta el nacimiento del ordenador, cuando aparece un mayor interés en estos. Dándose el caso curioso de algún dispositivo, como el cilindro de Bazeries, que con pocas variaciones sobrevive hasta mediados del siglo XX.

Criptógrafo de Wheatstone.

El físico ingles Charles Wheatstone (1802-1875), aparte de crear uno de los métodos más originales de cifrado, el de playfair, desarrolló un dispositivo similar al disco de Alberti. El criptógrafo de Wheatstone, presentado en 1867, consistía en dos discos concéntricos de los cuales el exterior tenía las 26 letras del alfabeto inglés en orden alfabético más el espacio en blanco y el interior las 26 letras del alfabeto totalmente desordenadas. El dispositivo tenía dos manecillas de diferente tamaño como las de un reloj, cada una de las cuales apuntaba a uno de los dos discos. El cifrado empezaba poniendo las dos manecillas apuntando al espacio en blanco del circulo exterior. Posteriormente se colocaba la manecilla exterior en la primera letra a cifrar, esto activaba los engranajes y posicionaba la manecilla interior en otra letra que correspondía al carácter cifrado. Esto se repetía con todas las letras de la primera palabra. Para cifrar cada una de las siguientes palabras se volvía a posicionar las dos manecillas en el espacio en blanco y se procedía como con la primera palabra.

Cilindros de Bazeries y Jefferson.

Los cilindros de Bazeries(1846-1931) y Jefferson (1743-1826) son sistemas que funcionan mediante la rotación de una serie de anillos numerados fijados a un eje formando un cilindro. Cada anillo tiene grabadas las letras del alfabeto en un orden diferente. La diferencia entre ambos es el número de anillos que lo forman, 20 con 25 letras en cada anillo en el caso del de Bazeries, y 36 en el de Jefferson. Para cifrar, el emisor y el receptor del mensaje se ponían de acuerdo en el orden en el que se iban a colocar los anillos. Una vez colocados, se escogía una fila y se hacía girar los anillos hasta que formase el mensaje a cifrar, luego simplemente se escogía cualquiera de las otras líneas y se enviaba al destinatario. El receptor del mensaje hacía girar los anillos de forma que una de las líneas coincidiese con el mensaje cifrado, luego giraba el cilindro hasta encontrar el mensaje en claro.



Este dispositivo, en varias formas, fue utilizado hasta la mitad de la segunda guerra mundial. En particular fue muy utilizada por el ejército (M-94) y la armada americanas (CSP-488) una versión de 25 cilindros desarrollada por el Coronel Parker-Hitt.

La gran ventaja de este dispositivo era su gran sencillez y la gran cantidad de posibles combinaciones que podía formar lo que prácticamente imposibilitaba el criptoanálisis manual. En particular existen $n!$ permutaciones de los anillos, siendo n el número de anillos del dispositivo.

Cifrado de Vernam.

Gilbert Vernam (1890-1960) desarrolló un método de cifrado para su utilización en los teletipos. El método consistía en la utilización conjunta de dos cintas en el teletipo de forma que su combinación fuera ininteligible, para ello utilizó la O exclusiva como operación de combinación de las dos cintas. La ventaja de esta operación es que el proceso de cifrado y descifrado es el mismo, variando únicamente la cinta a utilizar. El cifrado de Vernam es la base de un sistema perfecto de cifrado en el que se dispone de una cinta con una clave aleatoria tan larga como el mensaje a cifrar y que no se puede repetir jamás. Este método es conocido con el nombre de *one time pad*.

DAV96 A World War II german radio army field cipher and how we broke it. Charles David. Cryptologia Vol. XX nº 1. Enero 1996.

GAL95 Criptografía. Historia de la escritura cifrada. Juan Carlos Galende Diaz. Editorial Complutense.

LAS98 La France gagne la guerre des codes secrets. Sophie de Lastours. Tallandier 1998.

NEW98 Encyclopedia of cryptology. David E. Newton. ABC-CLIO 1998.

ROD86 Protección de la información. Diseño de criptosistemas informáticos. A. Rodriguez Prieto. Ed. Paraninfo 1986.

SAC51 Manuel de cryptographie. Général L. Sacco. Payot 1951.

SGA90 Códigos secretos. Andrea Sgarro. Pirámide 1990.

SIN00 Los códigos secretos. Simon Singh. Editorial Debate 2000.

TIM96 El tercer Reich. La guerra en la sombra. TIME LIFE 1996.