

CRIPTOGRAFÍA; DEFINICIONES.—SISTEMA DE «TRANSPOSICIÓN». —SISTEMA DE «PERTURBACIÓN».—DICCIONARIOS CIFRADOS.—CLAVE SILÁBICA DE CARMONA.—CRIPTOGRAFOS.—DESCIFRAMIENTO DE CRIPTOGRAMAS.

En tiempo de guerra, y muchas veces en el de paz, es necesario que las autoridades pueden comunicarse sin que nadie más que los interesados conozca el contenido de los telegramas. El arte de la escritura *secreta* ó *cifrada* se llama *Criptografía*. Es conocido desde tiempos muy antiguos y ya lo emplearon los griegos y romanos. En la Edad Media los monjes y cabalistas se valieron con frecuencia de ella y también lo han usado y usan las sociedades secretas. Según parece, en España la escritura secreta empezó á usarse oficialmente en tiempo de los reyes católicos. En los ejércitos empezó á usarse en el siglo XVII; pero hasta el actual no ha adquirido gran desarrollo; el empleo del telégrafo eléctrico ha hecho casi indispensable el uso de la criptografía, pues de lo contrario los telegrafistas se enterarían de los telegramas que expiden y reciben. Por esto hoy se da más importancia en el ejército á la criptografía que en Alemania forma parte del programa de las escuelas militares.

Según M. Kerschofs todo sistema de criptografía militar ha de cumplir las siguientes condiciones:

- 1.<sup>a</sup> Ser material, ya que no matemáticamente indescifrable.
- 2.<sup>a</sup> No ha de exigir secreto, ni importar que el enemigo lo conozca.
- 3.<sup>a</sup> La clave ha de poder comunicarse y retenerse sin auxilio de escritura alguna y modificarse á voluntad de los corresponsales.
- 4.<sup>a</sup> Es necesario que sea aplicable á la correspondencia telegráfica.
- 5.<sup>a</sup> Debe ser portátil y no exigir mucho personal para el desciframiento.
- 6.<sup>a</sup> Ha de ser de uso fácil, no exigir demasiada concentración de espíritu, ni el conocimiento de muchas reglas.

El telegrama en el cual se emplean signos convencionales para representar las palabras, sílabas ó letras del texto se llama *cifrado* ó *criptograma*.

Los procedimientos criptográficos que se empleen pueden agruparse en tres sistemas: 1.º Los que se originan transponiendo las letras del texto verdadero; es decir, variando su colocación. 2.º Los que substituyen las letras del texto verdadero por otras que resultan de cambiar, con arreglo á un convenio hecho de antemano, el orden alfabético. 3.º Los que representan las frases, las palabras, sílabas ó letras por grupos de letras ó cifras.

A los primeros sistemas les llama el señor Carmona de *transposición* y á los segundos de *perturbación*; pero en rigor perturbación la hay en todos.

Dentro de cada uno de estos sistemas puede seguirse diferentes procedimientos para cifrar los despachos, y estos procedimientos se llaman *métodos*. Además, para cifrar un despacho hay que hacer uso de una palabra, número ó frase convenida que se llama *clave*.

*1er sistema.* Uno de los métodos de este sistema consiste en escribir el contenido del telegrama al revés y transmitirlo luego; pero este método es muy elemental y fácilmente puede ser descifrado.

Otro método es el de simple transposición que consiste en escribir las letras del telegrama según el orden en que se hallan y de modo que formen una serie de líneas horizontales de igual número de letras; después se escriben según la misma disposición y en un orden cualquiera, representando cada letra de la primera línea horizontal por una cifra; el conjunto de estas cifras forman un número que es la clave. Sea, por ejemplo, el siguiente telegrama:

*El enemigo ha emprendido la retirada.*

	1	2	3	4	5	6	7	8
1	E	l	e	n	e	m	i	g
2	o	h	a	e	m	p	r	e
3	n	d	i	d	o	l	a	r
4	e	t	i	r	a	d	a	x

Para que todas las líneas horizontales resultaran con igual número de letras ha sido preciso añadir una al telegrama verdadero; ésta puede ser cualquiera y en general conviene que sea de las menos usuales. Esta circunstancia se presentará con frecuencia y algunas veces serán varias las letras que habrá que añadir. Estas letras, y en general todos los signos que no corresponden á ninguno del texto, se llaman *nulos* y dificultan el desciframiento.

El despacho anterior puede transmitirse como sigue:

1	5	3	4	8	1	6	7	2
	e	e	n	g	e	m	i	l
2	m	a	e	e	o	p	r	h
3	o	i	d	r	n	l	a	d
4	a	i	r	x	e	d	a	t

*e e n g e m i l m a e e o p r h o i d r n l a d a i r x e d a t*

En este sistema puede también variarse el orden de las cifras que constituyen la columna vertical y entonces hay una doble transposición. Claro es que para descifrar el despacho es preciso conocer el número ó números que constituyen la clave. En el ejemplo anterior la clave sería 5 3 4 8 1 6 7 2; para descifrar el telegrama se formaría la tabla 2.<sup>a</sup> y de ella se pasaría á la primera. En vez de esto podrían tomarse dos claves 5 3 4 8 1 6 7 2 y 3 4 2 1; entonces se formaría la tabla siguiente:

	5	3	4	8	1	6	7	2
3	o	i	d	r	n	l	a	d
4	a	i	r	x	e	d	a	t
2	m	a	e	e	o	p	r	h
1	e	e	n	g	e	m	i	l

y el telegrama transmitido sería

*o i d r n l a d a i r x e d a t m a e e o p r h e e n g e m i l*

Otro método que también entra en este sistema consiste en dividir el texto verdadero en grupos de un cierto número de letras; dentro de cada grupo se da á cada á letra una cifra de orden y con las cifras de un mismo grupo se forma un número en el cual la colocación de las cifras indica el orden en que deben transmitirse las letras. Sea, por ejemplo, el despacho:

*La caballe ríano ha visto al enemigo.*

Dividiremos el telegrama en grupos de cuatro letras y debajo de cada letra colocaremos una cifra como á continuación se indica:

Laca	ball	ería	noha	vist	oale	nemi	goxz
3214	4123	3124	2143	1342	3212	1432	2341

El telegrama cifrado será

*c a l a a l l b r i e a o n a h v t i s l e o a n i e m z x g o*

Los despachos así cifrados no son difíciles de descifrar, pues difícilmente se evita que contengan algunas sílabas iguales á las del despacho y que sirvan de guía. Así en el criptograma anterior se reproducen sílabas del texto verdadero.

2.º sistema. En estos puede suceder que en todo el telegrama la clave sea la misma ó que varíe, y según se adopte uno ú otro procedimiento, se llaman sistemas de clave única ó múltiple.

A. *Clave única.* Este consiste en escribir las letras del alfabeto en un orden cualquiera y debajo en orden natural, y en vez de transmitir las del telegrama, transmitir las que les corresponden en el alfabeto modificado. Supongamos que se adopte el alfabeto que á continuación se indica.

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

El telegrama *el enemigo h. comprendido la retirada* se convertirá en

T R T C T Q A X S Z F, etc.

Para determinar el orden en que deben escribirse las letras del alfabeto puede tomarse una clave cualquiera y representarla por un número. Sea, por ejemplo, *Coruña*, dando á cada una de las letras una cifra que representa el orden que ocupan en el alfabeto, esta palabra estará representada por *2 4 5 6 3 1* y el alfabeto se escribirá

2	4	5	6	3	1
b	d	e	f	c	a
h	j	k	l	i	g
n	o	p	q	ñ	m
s	u	v	x	t	r
z					y

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

El telegrama anterior será

*c g c o c n k h q, etc.*

B. *Clave múltiple.*—En estos el orden del alfabeto transpuesto cambia para cada letra.

Para aplicar más fácilmente este método se han ideado varias tablas, y la más antigua de ellas parece ser la de Tritemio; aun cuando los franceses le atribuyen à Vigenère, en realidad, el inventor parece ser el primero. Dicha tabla es la que à continuación indicamos:

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

Para emplear esta tabla se elige una clave cualquiera y se divide el telegrama en grupos de tantas letras como tiene aquélla, empleando para cifrar la primera letra de cada grupo el alfabeto horizontal que empieza por la primera letra de la clave, para las segundas el que empieza por la segunda y así sucesivamente. Supongamos que la clave sea *Río* y el telegrama el antes expresado; se escribirá como sigue:

Ele	nem	igo	hae	mpr	end	ido	lar	eti	rad	a
Río	Río	Río	Río	Río	Río	Río	Río	Río	Río	Río

El criptograma será

*v s s f m b a ñ e*, etc.

Porta empleó otra tabla más sencilla; á continuación indicamos parte de ella.

A B	a	b	c	d	e	f	g	h	i	j	k	l	m
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
C D	a	b	c	d	e	f	g	h	i	j	k	l	m
	z	n	ñ	o	p	q	r	s	t	u	v	x	y
E F	a	b	c	d	e	f	g	h	i	j	k	l	m
	y	z	n	ñ	o	p	q	r	s	t	u	v	x

Empleando esta tabla, las letras del telegrama verdadero se reemplazan en el criptograma por las que se hallan encima ó debajo en los dos renglones de minúsculas del alfabeto elegido. Para designar el alfabeto se recurre como antes á una clave. Supongamos que éste sea la palabra *Betis* y el telegrama el anterior; para cada letra se tomará un alfabeto distinto: para la primera el que corresponde á la primera letra de la clave ó sea *A B*; para la segunda el de la segunda ó sea el *E F* y así sucesivamente; de modo que la letra *E* se substituirá por la *q*, la *l* por *v*, etc.

La tabla de Vigenère ha sido modificada por el almirante inglés Beaufort, quien le ha dado la forma que á continuación se indica. Para emplearla supongamos que se quiere transmitir el mismo telegrama con la misma clave. Se toma la primera letra del telegrama (*e*) en el primer alfabeto horizontal, se sigue la columna vertical correspondiente hasta encontrar la *R*, primera de la clave y se transmite la que ocupa el extremo de la columna horizontal correspondiente á esta última letra, es decir, la *ñ*, luego se toma también en el primer alfabeto horizontal la segunda letra del telegrama *l*, se desciende por la columna vertical hasta la *I*, segunda de la clave y se transmite la *x* y así sucesivamente.

Cuando no se tenga á mano ninguna de las tablas anteriores, puede em-

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

plearse el método de Grimfeld. Para explicarlo con más claridad, lo haremos por medio de un ejemplo. Se toma por clave un número cualquiera, 374251, y se escribe debajo del telegrama tantas veces como quepa.

El enemigo ha emprendido la retirada  
 37 4251374 25 1374251374 25 13742513

Hecho esto, se transmite la letra del alfabeto que dista de la del telegrama tantos lugares como unidades tiene la cifra situada debajo. Así por ejemplo, en vez de *e*, se transmitirá *h*, en vez de *l*, *r*, en vez de la segunda *e*, *i*, etcétera.

Para que estos telegramas sean más difíciles de descifrar, en vez de repetir los alfabetos con regularidad pueden repetirse irregularmente, deteniéndose en una letra cualquiera de la clave y volviendo á empezar. Con objeto de que la persona á quien va dirigido el telegrama pueda descifrarlo, cada vez que se interrumpe la sucesión regular de los alfabetos, se transmite

una de las letras de la clave, y cuando esta letra no desempeña este papel sino que forma parte del telegrama, se substituye, á fin de evitar confusiones, por una cifra cuyas unidades indiquen el lugar que aquélla ocupa en la clave. Sea esta *Cisneros* y elijamos la *n* para indicar las interrupciones de la clave; entonces en el texto del telegrama se substituirá por *4*. Vamos á poner un ejemplo, tomando por base la tabla de Beaufort.

El batallón ha agctado las municiones.

Ci Cisneros Ci snerosC Cis cisnerosCi.

*y x N b i z 4 s h a g N u i N s h o y o p n N q i a N 4 g f c k a g y o*

Añadiendo delante de la primera letra otras nulas, separadas de aquella por un signo convencional cualquiera, se dificultará la traducción; el telegrama anterior podrá empezar, por ejemplo,

*h p q q w y x, etc.*

DICCIONARIOS CIFRADOS.—Estos consisten en un libro que contiene una serie de palabras ó frases numeradas. Para transmitir telegramas cifrados se pueden seguir diferentes procedimientos; uno de ellos ideado por Mr. Brunswick es el siguiente: supongamos que haya que transmitir la frase correspondiente al número 3415; se empieza por trasponer las cifras conforme á una regla de antemano convenida; sea por ejemplo, colocar en el centro las de los extremos y aquéllas en estos, se tendrá 4351; añádase á este número otro también designado de antemano 857;  $4351 + 857 = 5208$  será el número transmitido. Este sistema tiene varios inconvenientes. 1.º El enemigo puede apoderarse del diccionario por medio del dinero ó de la fuerza. 2.º Si el diccionario se pierde ó no se tiene á mano, no se pueden traducir los telegramas; tal sucedió en la campaña de 1870-71 en el cuartel general de von Werder en que un telegrama cifrado no pudo traducirse al recibirlo por no tener á mano el diccionario. En la guerra turco-rusa no pudieron traducirse en el cuartel general de Mehemet-Alí los telegramas recibidos durante la ausencia de Selím Bajá, quien se llevó por equivocación el diccionario. 3.º Es muy fácil equivocarse en la transmisión de números. 4.º Poseyendo un diccionario no le es difícil al enemigo, como luego veremos, la traducción de los despachos. Este sistema es, pues, inaceptable en campaña.

CLAVE SILÁBICA DE CARMONA.—Este oficial del ejército español propone un método criptográfico que realmente reúne muy buenas condiciones. Consiste en formar un cuadro ó tabla en donde se hallen por orden alfabético todas las sílabas del idioma en que han de escribirse los despachos; á la cabeza de cada grupo de sílabas que empiezan por la misma letra va escrita ésta en caracteres muy visibles, y al final de las sílabas las cifras y los sig-

nos ortográficos más usuales. A la derecha de cada letra, sílaba, guarismo ó signo se deja un claro en que se escribe un número cualquiera de tres cifras, es decir, desde 000 á 999. A las letras ó sílabas que más se repiten se les puede asignar dos ó tres números. Al cuadro así formado, y del cual damos á continuación una pequeña muestra, le llama *clave cifradora*.

*Clave cifradora Carmona.*

A.	. . . .	023
ab.	. . . .	001
ac.	. . . .	189
ad.	. . . .	475
ae.	. . . .	010
af.	. . . .	872
ag.	. . . .	002
ah.	. . . .	597
»	. . . .	»
»	. . . .	»
»	. . . .	»

Para pasar del criptograma al texto verdadero hay otra tabla llamada *clave descifradora*, en la cual están los mil números comprendidos desde 000 á 999 escritos de menor á mayor, y á la derecha de ellos claros para escribir las sílabas, letras ó cifras que les correspondan.

*Clave descifradora Carmona.*

000	034	068	100	134	168
001	035	069	»	»	»
002	036	070	»	»	»
003	037	071	»	»	»
004	038	072	»	»	»
005	039	073	»	»	»
006	040	074	»	»	»
007	041	075	»	»	»
»	»	»	»	»	»
»	»	»	»	»	»
»	»	»	»	»	»
»	»	»	»	»	»
»	»	»	»	»	»
033	067	099	133	167	199

Para completar este procedimiento hay que poner de acuerdo ambas claves, es decir, que en las dos han de corresponder á las sílabas, letras, etc., los mismos números. Hecho esto se divide en sílabas el texto verdadero, en su

lugar se transmiten las cifras que les corresponden y al recibirlas se pasa por medio de la clave descifrador de las cifras á las sílabas. Este método es realmente práctico é ingenioso, aplicable á la telegrafía, no exige mucho tiempo ni personal, ni hay que recordar reglas, ni claves. Tiene el inconveniente de que sea por extravío, sea por otra causa cualquiera, el enemigo puede adquirir las claves cifradora y descifrador.

Al emplear las tablas del señor Carmona, hay que tener en cuenta las siguientes observaciones: 1.<sup>a</sup> Los diptongos y triptongos se consideran como dos ó tres sílabas; *bien* se descompone como sigue *bi, en, buey; bu, e, y*. Se exceptúan de esta regla las sílabas *gue* y *que* en que la *u* no se pronuncia. 2.<sup>a</sup> La doble *r* se descompone, uniendo una á la vocal que la precede y otra á la siguiente. 3.<sup>a</sup> La *x* se une siempre á la vocal que la precede. 4.<sup>a</sup> En las palabras extranjeras se efectuará la división en sílabas de modo que pueda aplicarse dicha tabla.

CRIPTOGRAFOS.—Estos son aparatos ó disposiciones que trasponen ó perturban el orden de las letras, sílabas ó signos del telegrama. El *escitalo* de los lacedemonios puede reputarse como el criptógrafo más antiguo; consistía en un cilindro de madera ó marfil, al cual se arrollaba el papiro ó pergamino, y hecho esto, se escribía el telegrama en renglones que seguían la dirección de las generatrices. Se enviaba luego á la persona que debía leerlo, para lo cual había que arrollarlo á un cilindro igual. Como se ve, el procedimiento es bastante primitivo.

Eneas el táctico, ideó una tablilla con 24 agujeros que representaban las letras del alfabeto, dichos agujeros estaban numerados, y por ellos se hacía pasar un cordel; el orden en que los atravesaba indicaba el de las letras del alfabeto empleado.

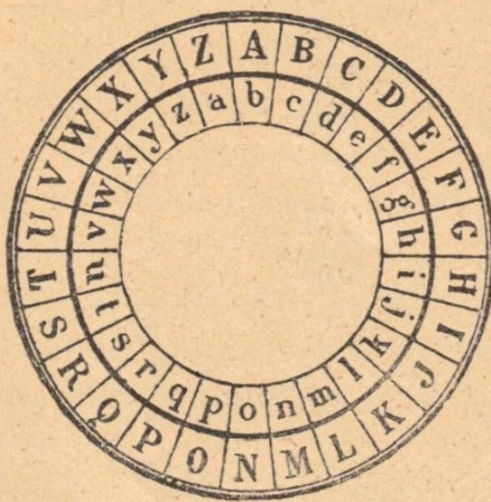


Fig. 286

Porta ideó, en 1583, un criptógrafo formado por dos círculos concéntricos (figura 286), uno con el alfabeto en su orden natural, otro con el alfabeto en orden cualquiera; este segundo disco podía girar al rededor de su eje. Para

emplear esta disposición basta colocar el disco interior de modo que cada una de sus letras corresponda á otra del exterior y buscar las que en aquél corresponden á las del telegrama escritas en éste. En la disposición de la figura el telegrama:

«El batallón ha agotado las municiones»  
se escribirá:

*f m c b u b m m p o, etc.*

Si se quiere seguir el sistema de clave variable, basta mover el disco interior después de haber transmitido cada una de las letras.

El criptógrafo de Wheatstone es una modificación de este procedimiento; consta también de dos discos, el exterior está recorrido por una aguja larga que indica las letras del telegrama, y las que se transmiten son las marcadas en el interior por otra aguja más corta. Para cambiar la correspondencia entre ambos discos, el aparato está dispuesto de modo que después de haber dado la aguja larga una vuelta completa, la corta haya dado  $\frac{28}{27}$  de vuelta; suponiendo que el criptógrafo tenga 27 sectores. Para descifrar los telegramas hay que conocer el ángulo que forman las agujas al principio de la transmisión. El procedimiento empleado en la escuela de Saint Cyr, para la formación de telegramas secretos, es un verdadero criptógrafo. Consiste en una re-

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	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	c	d	e	etc.
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	------

gla fija, que contiene el alfabeto natural y otra que corre á lo largo de ella y lleva un doble alfabeto también ordinario. La clave debe ser una palabra de tres á cinco letras. El telegrama se divide en grupos de tantas letras como tiene la clave. Sea por ejemplo esta *Fusil* y el telegrama:

«Salen refuerzos.»

Se corre la regla inferior hasta que la letra *F*, primera de la clave, se halle debajo de la *A* de la regla fija y se transmite en vez de las primeras letras de los grupos, las que les corresponden en el alfabeto superior; se corre luego la reglita hasta que *u* segunda letra de la clave, caiga debajo de *A* y se transmiten las letras que en el alfabeto superior corresponden á las segundas de cada grupo, y así sucesivamente. Pueden reemplazarse las reglas por tiras de papel cuadriculado. Este procedimiento no es más que una modificación de la tabla de Vigenère, pero tiene la ventaja de que es más fácil de disponer y usar. A su vez el criptógrafo de Wheatstone, es una transformación de la regla usada en la escuela de Saint Cyr.

Parecido el procedimiento de Saint Cyr es el usado en nuestro Ministerio de la Guerra.

En una cuartilla de papel se escribe el alfabeto normal; debajo de él se hace correr una cinta que contiene un doble alfabeto perturbado con arreglo á una clave cualquiera. Debajo de la cinta se forma un encasillado con tantas casillas horizontales como tiene el alfabeto y siete verticales; de modo, que, debajo de cada letra hay siete casillas verticales, y en tres ó cuatro de éstas se ponen números, dejando las demás vacías. Para usar este encasillado se hace coincidir una letra de la cinta con otra del alfabeto fijo, se transmiten estas dos letras al que ha de descifrar, se leen en la cinta las letras del telegrama verdadero, y en vez de éste se transmite uno de los números que hay debajo. En el cuadro adjunto el alfabeto perturbado lo ha sido tomado por clave la palabra *Lancero* con lo cual resulta:

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

á fin de que la perturbación sea mayor, ordenaremos las letras por columnas verticales, con lo cual resulta el adjunto alfabeto:

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

y haciendo coincidir la letra *f* de la cinta móvil con el alfabeto, fijo tendremos el adjunto cuadro en el cual puede verse que sólo se emplean 90 números, desde el 10 al 99, y se hallan ordenados horizontalmente:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	X	Y	Z	
<i>n</i>	<i>f</i>	<i>ñ</i>	<i>x</i>	<i>c</i>	<i>g</i>	<i>p</i>	<i>y</i>	<i>e</i>	<i>h</i>	<i>q</i>	<i>z</i>	<i>r</i>	<i>i</i>	<i>s</i>	<i>o</i>	<i>j</i>	<i>t</i>	<i>l</i>	<i>b</i>	<i>k</i>	<i>u</i>	<i>a</i>	<i>d</i>	<i>m</i>	<i>v</i>	<i>n</i>	<i>f</i>
				10				11					12	13								14				15	16
			17			18			19								20						21	22	23	24	25
	26	27				28					29	30							31	32			33		34		
	35		36	37	38							39				40	41				42			43		44	
		45		46	47			48	49	50		51	52	53	54	55		56		57			58			59	
	60	61		62		63	64	65		66	67		68	69	70	71	72	73		74	75	76		77	78		
	79		80		81	82	83	84	85	86	87	88	89	90	91		92	93	94	95	96	97	98	99			

Según este cuadro, la clave está dada por las letras *A*, *f*, y la palabra *General* se escribiría 38 49 16 11 88 21 73.

mos á dar reglas para ello, sino indicaciones acerca de la marcha que debe seguirse.

Facilitan mucho esta tarea el conocimiento del idioma en que se halla escrito el criptograma, el del asunto á que se refiere, el de las personas que lo remiten y reciben. Todos estos datos pueden algunas veces averiguarse con certeza, otras sólo por medio de indicios.

Conviene mucho fijarse en la proporcionalidad en que entran las letras del alfabeto, pues claro es, que las del criptograma que más se repitan han de corresponder á las más usadas. En español se repiten muchas veces monosílabos tales como *me, te, se, le, el* en que entra la *e* como vocal, abundan mucho las terminaciones en *on* y las en *ido* y *ado*, que son características de los participios; la *u* y la *q* van juntas con mucha frecuencia, y la mayor parte de las sílabas de tres letras tienen en el centro una vocal; la letra final de las palabras que terminan en vocal suele ser *a* ú *o*, características del género, y la *s*, característica del plural, es también una terminación frecuente.

Según el señor Carmona, la importancia de las letras del alfabeto español y el tanto por mil que corresponde á cada una, es el que á continuación se indica:

E	A	O	N	S	I	R	L	D	C	T	U	P	M	G	B	Y	V	F	J	Q	Z	H	X	Ñ	K	W
146	119	91	72	72	71	66	55	50	48	46	33	31	28	13	11	11	9	7	6	5	4	3	2	1		

Según Mr. Vesin la importancia de las distintas letras en varios idiomas es la que se indica en el cuadro adjunto.