ORGANICA NAVAL

Con un compendio completo de Criptografía

Por el Capitán de Corbeta (Diplomado de Estado Mayor)

PASCUAL DIEZ DE RIVERA Y CASARES

Sub - Director (interino) de la Escuela de Guerra Naval
y Profesor de Orgánica y Derecho Internacional Marítimo en este Centro

M A D R I D 1 9 3 4

CAPITULO IX

CRIPTOGRAFIA

Definiciones.—Alfabetos varios.—Claves y Métodos.—Tablas de frecuencia del idioma.—Métodos de sustitución y de trasposición o perturbación.—Diversos sistemas.—Máquinas para cifrar.-Criptoanálisis furtivos.—Códigos.—Claves silábicas.—Ventajas e inconvenientes de unos y otros sistemas.—Normas a tener en cuenta para cualquier cifrado.—Condiciones esenciales de todo buen descifrador y de todo método criptográfico.

Criptografía. – Definiciones. – Alfabetos diversos.

Criptografía es la ciencia de cifrar. Comprende todos los métodos científicos y artes materiales utilizables para que una comunicación o mensaje claro e inteligiblemente escrito, sea puesto de manera que sólo lo pueda interpretar la persona a quien va dirigido y resulte comunicación secreta para los demás.

La idea de que lo que uno quiera expresar escribiendo a otra persona no lo comprenda más que ésta, es tan antigua como la escritura misma.

Si la escritura es la representación material de la palabra, se comprende que la escritura desfigurada es la representación de la palabra o de los gestos desfigurados; por ello se asegura que la criptografía es tan antigua como la existencia de la Humanidad. En donde primero se empleó fué en asuntos de amor, que son los primeros negocios que se entablaron y de que se tiene noticias; por tanto, la criptografía es tan antigua como el hombre mismo.

El lenguaje de las flores, el del abanico, el del pañuelo, el del bastón, la escritura con tinta simpática etc., etc., son otras tantas estratagemas usadas para comunicarse secretamente unos con otros, y todas estas habilidades forman parte de la criptografía.

Los geroglíficos de los egipcios, los signos aztecas o o incas y tantos otros, son representaciones que se usaban para expresarse en las civilizaciones primitivas, las más antiguas que se conocen; todo ello son ejemplos de escrituras

figurativas. El cifrado por medio de estos signos recibe el nombre de *Esteganografía.*

Pero dejando aparte el desenvolvimiento histórico de la Criptografía en general, no obstante su gran interés, nos concretaremos al estudio de la Criptografía militar.

Desde luego es más fácil inventar un sistema de cifrar un mensaje, que interpretar o descifrar un mensaje cifrado del que no conozcamos la clave ni su método.

Según Mr. Kerckhoffs, las condiciones generales que ha de reunir un Método Criptográfico son:

1.ª Debe ser material, sino matemáticamente indescifrable.

2.ª Es necesario que no exija el secreto pudiendo sin inconveniente caer en poder del enemigo.

3.ª La clave debe ser susceptible de poderse comunicar y retener sin necesidad de notas escritas y cambiarla o modificarla a voluntad de los corresponsales.

4.ª Debe poderse utilizar con el telégrafo.

5.ª Debe ser portátil y que su manejo no exija el concurso de varias personas.

6.ª Por último, vistas las circunstancias que exigen su aplicación es necesario que el método sea de uso fácil y sencillo que no necesite tensión de espíritu ni el conocimiento de muchas reglas que observar.

Dice Mr. H. Josse: "La Criptografía militar propiamente dicha debe emplear un sistema que no exija más que un papel y un lápiz."

En España se ha cultivado y con fortuna, antes más que ahora, el estudio sobre estas disciplinas; Carmona, Núñez, Losada y tantas otras obras ya agotadas, son una muestra de lo que decimos. Modernamente los jefes de los Gabinetes de Criptografía o los de las Secciones de Información en los Estados Mayores Centrales de la Gran Guerra han escrito obras sobre tan interesante tema, entre otras Lange y Soudart, y Giviérge nos legaron el fruto de sus estudios.

La Criptografía tiene aplicación, más que en otras actividades de la vida, en la Milicia, en la Diplomacia y en el Comercio.

El campo en que cada una de estas actividades opera y las condiciones en que se trabaja, marcan las características peculiares en el desarrollo de cada una de estas tres ramas en que se puede dividir la criptografía moderna.

La Criptografía Militar tiene características especiales, requiere gran práctica en quien la maneja. Desde luego, es indispensable en todos los escalones del Mando, desde los Estados Mayores Centrales hasta en los Mandos pequeños, y la premura con que se tendrá muchas veces que transmitir órdenes de inmediata puesta en práctica, exige en quien cifre y luego en quien descifre una práctica consumada que no es tan necesaria ni en la Diplomacia ni en lo Comercial.

El cifrar bajo la presión del enemigo hace que no se tenga la tranquilidad completa y el que opera así, dado el nerviosismo natural, nada tiene de extraño que se equivoque; con lo que tanto ha de dificultar la labor del que reciba e interprete el criptograma; si hay que pedir "repetición" ya comprenderemos cuánto dilatará los efectos que tiene que surtir esa orden y las consecuencias que ello pueda acarrear. Siempre hay poca comodidad en una tienda de campaña, en un destructor o submarino, no hay ni espacio ni grandes medios para trabajar con orden (cualidad primordial del criptógrafo). Además las "claves" deben ser reducidas y los "códigos" pocos, pues a lo mejor hay que abandonar la posición en que se opera y hay que llevar sobre sí los dichos documentos, o destruirlos para que no caigan en poder del enemigo.

En la Diplomacia es donde se puede con más facilidad emplear la Criptografía. Las oficinas en las cancillerías de Embajadas y Legaciones son locales amplios, cómodos y seguros de toda intromisión de personal extraño; permiten

emplear claves y códigos voluminosos y usar tantos como sean necesarios. La extraterritorialidad de los edificios en que se opera da una seguridad grande y en el caso de ruptura de relaciones de esa nación con otra, el diplomático podrá con toda garantía recoger sus papeles y sus códigos y consigo los llevará hasta pasar la frontera, pues, según las leyes del Derecho Internacional, el Gobierno debe respetarle y despedirle con todos sus honores. Además, los documentos diplomáticos, por su índole especial, la mayor parte de las veces, no requieren gran urgencia en el cifrado ni en el descifrado y ello permite una tranquilidad de espíritu en quien trabaja, que unida a la comodidad que en la oficina encontrará es la mayor garantía de que no habrá equivocaciones en el cifrado y ello facilita todo enormemente.

La Criptografía Comercial, también tiene sus características especiales. La Banca, el Comercio, etc., usan códigos especiales en los cuales la mayor parte de las veces, más que el secreto de la comunicación—que a veces puede ser requerido—, tienden a la economía de la transmisión telegráfica. Existen códigos internacionales que todo lo facilitan.

Para cifrar un mensaje cualquiera se requieren dos cosas, una clave y una manera o método de aplicar esta clave. El estudio de la Criptografía tiene dos partes:

La *criptografía* propiamente dicha, o sea cifrar un mensaje, que una vez en forma ininteligible se llama *criptograma.*

La *criptografía analítica* o criptoanálisis que permite descifrar el mensaje, esto es, traducirlo en forma inteligible para cualquiera.

Para cifrar un mensaje no se requieren dotes especiales; conociendo la clave y el método, cualquier individuo puede hacer un criptograma.

Para la *criptografía analítica furtiva,* esto es, para descifrar un criptograma sin conocer la clave ni el método, sí que se requieren dotes especiales, como son necesarios para

descifrar un jeroglífico, para acertar una charada o para resolver aquellos problemas de cálculo que ya se dominaban de "feliz idea", y que salían fácilmente sumándoles o restándoles una determinada cantidad; de la intuición de quien los trabajaba dependía el encontrar más o menos pronto esa cantidad, y como consecuencia, la apetecida solución. Al explicar la criptografía analítica insistiremos más sobre este tema.

Seguridad y sencillez.—En asuntos criptográficos son dos cualidades antagónicas. Para cifrar un mensaje, la clave más segura que no caerá nunca en manos del enemigo es una palabra que aprendamos de memoria, pero... si esta palabra *se nos olvida* todo caerá por su base. Cuanto más complicada sea la clave o código que empleemos y cuanto más a menudo lo variemos, más difícil será que nuestros criptogramas sorprendidos sean descifrados, pero también cuanto más complicado sea el método empleado para cifrar, más complicado será luego el descifrado; por ello decíamos que "seguridad y sencillez" en estos casos son cosas antagónicas; sin embargo, mediante el conocimiento y aplicación de reglas criptográficas ya veremos que se llega a un límite que sin ese estudio y conocimiento sería imposible de compaginar. Desde luego, se demuestra en criptografía analítica que la seguridad de un criptograma depende de la frecuencia con que se cambie la clave.

Todo cifrado consta de dos elementos: el sistema de cifrar o regla que seguimos, que se aplica constantemente sobre todo el criptograma y la clave con que trabajamos.

La *clave* es la convención que existe entre dos o más personas y solamente conocida por ellas, que permite transformar un texto ordinario en un criptograma o inversamente en un sistema establecido. Esta clave puede ser una palabra, una cifra numérica o una frase.

Hay en Criptografía dos sistemas fundamentales que se utilizan para cifrar.

a) Sistema de sustitución, que consiste en cambiar las letras del texto ordinario por otras.

b) Sistema de trasposición, que consiste en mezclar o trasponer las letras del texto ordinario, sin sustituirlas por otras.

Pero antes de seguir adelante, veamos los alfabetos que se emplean con más frecuencia en Criptografía.

Del alfabeto sólo usaremos 25 letras. Ello nos permitirá, por ser un múltiplo de 5, hacer un cuadrado completo de 5 líneas y 5 columnas que puede servir para diversas composiciones criptográficas. Las tres letras que suprimimos son la *ll*, la ñ y la *w*, que llamaremos "letras mudas". Nos servirán cuando hagan falta para rellenar huecos, como iremos viendo en el transcurso de estos estudios.

En Criptografía, los alfabetos se consideran escritos en círculo cerrado; no terminan; a la última letra, le sigue la primera.

Alfabeto normal es el alfabeto comúnmente empleado:

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

Alfabeto normalmente ordenado es el alfabeto normal que en vez de comenzar por la letra *A* empieza por cualquier otra siguiendo el orden creciente del normal:

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

es un alfabeto normalmente ordenado.

Alfabeto incoherente es aquel en que las letras se han colocado en cualquier orden.

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

Alfabeto recíproco es un alfabeto normal, normalmente

ordenado o incoherente, dividido en dos partes y colocado en dos renglones de tal modo que las letras del primer renglón sirven para cifrar las correspondientes del segundo y viceversa.

Ejemplo:

Empleamos 26 letras con objeto de tener un número par de letras; por ello incluímos la W.

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

B = O O = B

Alfabetos inversos son alfabetos recíprocos en que la primera del uno corresponde a la última del otro:

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

Los alfabetos recíprocos e inversos pueden ser normalmente ordenados o incoherentes.

Alfabetos complementarios son aquellos en que la suma de las letras correspondientes de los dos renglones da una suma constante.

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

I + Q = 9 + 17 = 26 G + S = 7 + 19 = 26 F + T = 6 + 20 = 26

Los alfabetos inversos son siempre complementarios.

Alfabetos paralelos son aquellos en que dos letras correspondientes de uno y otro renglón aparecen en cada alfabeto separadas por un número igual de letras:

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

Entre la O y la E en el primer renglón 5 letras.
Entre la L e Y en el segundo renglón 5 letras.

Alfabeto intervertido es el que se forma utilizando como base para su formación las letras de una palabra clave y colocando de bajo de ella las demás del alfabeto normal, por orden natural; no poniendo las que entren en la palabra clave:

Sea *navío* la palabra clave:
para formar el *alfabeto intervertido* se procede en la siguiente forma:

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

en diagonal sería:

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

en espiral:

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

también caben otras combinaciones: por líneas, por columnas, en zi-zag, etc.

Este alfabeto presenta la ventaja de que no hay que llevarlo escrito, basta con recordar de memoria la palabra que sea la clave, y en el momento necesario formamos nuestro cuadro y en seguida el alfabeto "intervertido" que además podemos variar cuando convenga.

Para emplear prácticamente la correspondencia de alfabetos, se forman unas tablas que se llaman "tableros de concordancia", que consisten en tener arriba escrito el alfabeto normal y debajo otro alfabeto que puede ser incoherente, intervenido, etc., de manera que se corresponda con aquel en la forma que nosotros deseemos; suelen escribirse estos alfabetos en discos concéntricos y al girar uno sobre otro variamos su "correspondencia".

Claves y métodos.

Ayer hablamos de los alfabetos, hoy nos ocuparemos algo de claves. Entendemos por tales los "convenios" que en un método cualquiera se adoptan para guardar el secreto.

Ya dijimos que todo "cifrado" consta de un sistema de cifras, esto es, una regla o método y una clave sobre que aquél se aplica. Esta clave puede ser una palabra, una cifra, un libro, una tabla, etc.

Las claves pueden ser limitadas o ilimitadas.

Las claves de letras pueden convertirse en numéricas y recíprocamente.

Veamos ligeramente algunos casos.

En la criptografía moderna, dado que los medios de trasmisión más rápidos son los telegráficos, para decir más cosas con menos palabras o signos, suele emplearse un libro, un código, pero también se usan frecuentemente palabras aisladas como base de una clave. Esta clave—una palabra—es la que más *encaja* en aquella condición necesaria para que la criptografía militar sea práctica; aquella que sólo decía exigir "un lápiz y un papel".

Si tomamos como clave un libro cualquiera, p. e., "Armada Española", de Fernández Duro (tomo I); veamos cómo se puede emplear.

Al empezar el cifrado daremos cinco números, que serán: los tres primeros la página y los otros dos la línea: 24114 (pág. 241, línea 14) "como el almirante..." tomaremos sus diez primeras letras

como el almi

y pondremos debajo de cada una los números del 0 al 9 por orden correlativo en que aquéllas ocupan en el alfabeto normal; si hay dos letras iguales no importa, le damos los números consecutivos para evitar la denuncia de la frecuencia del idioma, y resultará:

c o m o e l a l m i
1 8 6 9 2 4 0 5 7 3 esta será nuestra clave,

así convertimos las claves alfabéticas en numéricas, y recíprocamente.

Texto a cifrar: Hoy hace sol;
se une todo: h o y h a c e s o l ,
y de cada letra se toma su número de orden del abecedario general.

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

y se sustituye por la equivalencia de nuestra clave. Cuando por su lugar sea un número de una sola cifra se le antepone la letra que equivale al cero y resultará: la h es el número 8 en el alfabeto normal y en nuestra clave el 8 está representado por la letra O y como tiene una sola cifra le anteponemos la letra *a* que en dicha clave corresponde al cero, así es que: 08 la representamos por ao - siguiendo el texto a cifrar, diremos la *o* de "hoy..." es el número 15 del alfabeto normal y el número 15 en nuestra clave lo representamos por el cl... así es que el criptograma de "Hoy hace sol" estará representado por:

aoclelaoacaialcoclce.

Para el criptoanálisis se divide en grupos de 2 y se opera a la inversa.

Con un libro que alcance 1.000 páginas y cien renglones

por página, tendremos con cinco cifras cien mil claves (suponiendo ooo la pág. 1.000 y oo el renglón 100). Por otra parte, las permutaciones de las diez cifras dan 10! = 3.628.800 que satisface a las mayores exigencias.

Pero no siempre podemos llevar con nosotros el libro clave; veamos un método sencillo para retener en la memoria todas cuantas claves necesitemos en la práctica. Cojamos un dicho corriente de nuestra lengua y de fácil recordación: "Quien mucho habla mucho yerra", y escribámoslo en un cuadro con sus vértices numerados.

1				2
q	u	i	e	n
m	u	c	h	o
h	a	b	l	a
m	u	c	h	o
y	e	r	r	a
3				4

y empecemos a sacar claves:

4	horizontales	
4	verticales	
8	diagonales	(dos diagonales en cada punta)
8	en espiral	(dos en cada vértice)
8	en zig-zag	(dos en cada vértice)
Total	32	claves.

y como en cada una de estas claves se puede empezar por cualquier letra serán:

$$32 \times 25 = 800 \text{ claves.}$$

Cuatro por horizontales

Clave 121 - quienmuchohablamuchoyerraquien. . . . .
" 212 - neiuqohcumalbahohcumarreynei. . . . . .
" 343 - yerramuchohablamuchoquienyer. . . . . .
" 434 - arreyohcumalbahohcumneiuqarr. . . . . .

Cuatro por verticales

Clave 131 - qmhmyuuaueicbcrehlhrnoaoaqmh. . . . . .
" 242 - noaoaehlhricbcruuaueqmhmynoa. . . . . .
" 313 - ymhmqeuauurcbcirhlheaoaonymh. . . . . .
" 424 - aoaonrhlhercbcieuauuymhmqaoa. . . . . .

Ocho en diagonales

Clave 132 - qmuhuimaceyubhneclorharoaqmu. . . . . .
" 123 - qumiuhecamnhbuyolceahroraqum. . . . . .
" 214 - neoihaucloqubhamacrhurmeyneo. . . . . .
" 241 - noeahiolcuahbuqrcamruhemynoe. . . . . .
" 314 - ymehurmacrqubhaucloihaeonyme. . . . . .
" 341 - yemruhrcamahbuqolcuahioenyem. . . . . .
" 432 - arorhaecloyubhnmacehuimuqaro. . . . . .
" 423 - aorahrolcenhbuyecamiuhumqaor. . . . . .

Ocho en espirales

Clave 124 - quienoaoarreymhmuchlhcuabqui. . . . . .
" 134 - qmhmyerraoaoneiuuauchlhcbqmh. . . . . .
" 243 - noaoarreymhmquiehlhcuaucbnoa. . . . . .
" 213 - neiuqmhmyerraoaohcuauchlbnei. . . . . .
" 312 - ymhmquienoaoarreuauchlhcbymh. . . . . .
" 342 - yerraoaoneiuqmhmuchlhcuabyerr. . . . . .
" 431 - arreymhmquienoaohcuauchlbarr. . . . . .
" 421 - aoaoneiuqmhmyerrhlhcuaucbaoa. . . . . .

Ocho en zig-zag

Clave 122 - quienohcumhablaohcumyerraqui. . . . . .
" 133 - qmhmyeuauuicbcrrhlhenoaoaqmh. . . . .
" 211 - neiuqmuchoalbahmuchoarreynei. . . . . .
" 244 - noaoarhlheicbcreuauuqmhmynoa. . . . . .
" 344 - yerraohcumhablaohcumquienyer. . . . . .
" 311 - ymhmquuauercbciehlhraoaonymh. . . . . .
" 433 - arreymuchoalbahmuchoneiuqarr. . . . . .
" 422 - aoaonehlhrrcbciuuaueymhmqaoa. . . . . .

Como dijimos, cada una de estas claves es susceptible de empezarla por la letra que deseemos, siempre que se indique, por ejemplo:

clave 12104, quiere decir que tomamos la 1.ª clave y la letra primera será la e:

enmuchohablamucho...

tomamos sus diez primeras letras, pongamos por caso, y dividimos esas diez letras en dos grupos de a 5,

enmuc - hohab

las numeramos como en el ejemplo anterior

e n m u c - h o h a b
1 3 2 4 0 - 2 4 3 0 1 esta es la clave

y vamos a cifrar

Salga escuadra a media noche

dividimos la frase en grupos de 5 letras y numeremos sus letras de 0 a 4:

S a l g a e s c u a d r a a m e d i a n o c h e x
0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4

escribamos los números de la clave en cuadro así:

- Clave 12104 -

e n m u c - h o h a b

1 3 2 4 0 2 4 3 0 1

	2	4	3	0	1
0	l	a	g	s	a
4	h	x	e	o	c
2	a	m	a	d	r
3	i	n	a	e	d
1	c	a	u	e	s

0	1	2	3	4
salga	escua	dra a m	edia n	oche x
01234	01234	012 3 4	0123 4	0123 4

Una vez hecho este cuadro, el orden en que se coloquen las letras al sacarlas de él para formar el criptograma y poner el telegrama se puede emplear cualquiera de los 32 explicados, pero en ese caso tendría que ponerse la clave si no estaba convenida y de no decirse nada creemos que debe ser la de los tres primeros números, en este caso la 121 (cuatro por horizontales) y se pondría así el telegrama:

l a g s a h x e o c a m a d r i n a e d c a u e s

Para el desciframiento se procede en orden inverso.

A continuación damos, como nota curiosa, una serie de refranes de 25 letras cada uno.

El buen paño en el arca se vende.
A la res vieja, alíviale la reja.
Cada gallo canta en su muladar.
Más vale un toma que dos te daré.
Ira de hermanos, ira de diablos.
Donde vayas de los tuyos hayas.
Gloria vana, florece y no grana.
Hombre prevenido vale por dos.
No hay mal que por bien no venga.
Lo cortés no quita lo valiente.

Olivo y aceituno, ¿no es todo uno?
La cabra siempre tira al monte.
Con el tiempo maduran las uvas.
Cuales barbas, tales toballas.
Sobre un huevo pone la gallina.
Más vale la fama que la riqueza.
Pasión no quita conocimiento.
Dios los cría y ellos se juntan.
El mal sea para quien lo quiera.
Bien vengas mal, si vienes solo.
Pobre porfiado saca mendrugo.
De zuma a zumarra poco se marra.
Una golondrina no hace verano.
A padre ganador, hijo gastador.

Tablas de frecuencia del Idioma. Método de Julio César. – Sistema de simple sustitución a simple, doble y múltiple representación.

Ya dijimos que para cifrar se emplean dos grandes sistemas: el de sustitución y el de transposición.

El primero se sustituyen las letras del texto por signos que en general son cifras (letras o números).

El segundo emplea las mismas letras del texto claro, alternándolas.

Hablemos un poco de nuestras letras y de las "Tablas de frecuencia".

La base para interpretar furtivamente los criptogramas consiste en un estudio profundo sobre la proporcionalidad en que entran las letras en nuestro idioma, su tanto por ciento o sea número de veces que se repiten; esto se llama la "ley de frecuencia".

Los trabajos hechos sobre el idioma español por Carmona y Núñez no coinciden exactamente, pero como las diferencias no son grandes y los de este último son posteriores a los de aquel, tomamos los datos de los estudios efectuados por Núñez.

A medida que los años pasan se van introduciendo en los idiomas algunas diferencias en el empleo de ciertas palabras y algo hacen cambiar las tablas de frecuencia; pero es tan pequeña esa variación que los estudios hechos sobre una lengua determinada pueden aplicarse con eficacia durante períodos larguísimos de tiempo.

En 100.000 letras tomadas de obras de nuestros clásicos

Cervantes, Fray Luis de León, Quevedo, Solís, Alarcón, Balmes, etc., resultan las letras repetidas en la proporción siguiente: por 1.000.

E	A	O	S	N	R	I	L	D	U	T	C
132,99	126,41	93,50	78,20	68,14	64,05	63,42	55,31	49,72	42,77	41,43	40,61
M	P	B	Y	G	Q	V	H	F	J	Z	Ñ
28,49	25,04	14,47	12,13	11,98	11,61	10,56	9,32	7,13	4,68	4,37	2,13
X	W	K									
1,37	0,09	0,08									

Hay hechos estudios sobre bigramas, trigramas, sílabas y aun frases corrientes, palabras que empiezan por una misma letra, orden por que las letras se repiten, tanto por ciento de todo ello, etc., etc., y se representan por curvas que facilitan grandemente el descifrado furtivo de un criptograma.

En estas 100.000 letras citadas hay 21.594 palabras y, por tanto, cada palabra sale a 4,63 letras. De estas 21.594 palabras tenemos 1.523 de una letra en la proporción siguiente:

Y	A	C	E	U
894	503	112	13	1

La terminación más frecuente de palabras es *o, a, s;* es natural, pues corresponden a las terminaciones masculinas, femeninas y a los plurales.

Asimismo es muy frecuente en nuestro idioma las terminaciones en

mente, ísimo, ción y fico.

Los grupos de tres letras en palabras sueltas, como "que",

"con", "sin", dan luces indudables para el descifrado furtivo, así como el que las vocales y consonantes van casi siempre alternadas. A la *q* le sigue siempre la *u*. Pero no es nuestro idioma de los que tienen más letras forzadas para sucederse. En idiomas extranjeros sucede eso con mucha mayor frecuencia.

El idioma español, como de origen latino, es riquísimo en palabras, y ello complica sobre manera el descifrado furtivo de los criptogramas. Los idiomas de origen sajón se pueden hablar bien con la quinta parte de las palabras de los latinos. Y aseguran los que conocen los idiomas orientales, como el chino y el japonés, que el reducido número de guarismos que se emplea en su escritura y las pocas palabras relativamente que se usan en la conversación corriente han hecho que mensajes cursados en aquellos idiomas no hayan sido tan difíciles de descifrar, a los competentes en ello, como a primera vista pudiese parecer. Durante la guerra pasada hay ejemplos de todo; se recurrió a lo inverosímil para que los servicios de espionaje pudiesen mantener sus comunicaciones en secreto.

El *sistema de sustitución* puede ser a simple o a doble clave. El primero es el que utiliza un solo alfabeto o "tablero de concordancia", que es la clave. El segundo sistema es el que utiliza dos o más alfabetos o tableros de concordancia, o también una palabra clave y un tablero, etc.

Por ejemplo, deseamos cifrar: *necesito petróleo.*

El sistema más antiguo que se conoce es el de Julio César, que es del tipo primero; empleaba un alfabeto decalado con el normal un cierto número de letras. Por ejemplo:

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

el criptograma que deseamos sería:

mensaje = n e c e s i t o p e t r o l e o
criptograma = l c a c q g r m n c r p m j c m

Es un método que no da ninguna garantía de seguridad; la frecuencia de las letras del texto claro se manifiesta íntegramente en el criptograma: 4 e representadas por 4 c; 3 o representadas por 3 m.

Para descifrar estos criptogramas basta con poner el texto capturado y escribir verticalmente debajo de cada letra las que se siguen en el alfabeto normal, hasta leer claro el texto:

l c a c q g r m n c r p m j c m
m d b d r h s n o d s q n k d n
n e c e s i t o p e t r o l e o

al tercer golpe salió el mensaje claro.

Podría complicársele dividiendo el texto en grupos y metiéndole letras mudas y cifrarlo luego con varios alfabetos decalados distinto número de lugares, pero ya dejaría de ser de sustitución a simple clave.

Para eliminar la frecuencia se puede complicar la sustitución simple dando doble o triple representación a cada una de las letras del texto ordinario. Nos bastará con confeccionar un cuadro de valores.

Así:

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

y cada letra del texto ordinario la sustituímos por el bigrama que se forma tomando las dos letras de las puntas de las filas que concurren en ella. Por ejemplo, si queremos cifrar la palabra

a g u a

el criptograma sería (1.° la vertical, y luego, la horizontal).

b a c e b u b a

o también:

a b e c u b a b (1.° la horizontal, y luego, la vertical).

La clave es el cuadro, el sistema es de simple sustitución, a simple clave y doble representación. Algo más complica el criptograma, pero tiene el gran defecto de que se duplica el número de letras del texto claro, y que la frecuencia del idioma sigue manifestándose.

Para complicar los criptogramas hay que procurar eliminar la frecuencia del idioma, y esto se consigue dando doble, triple o cuádruple representación a las letras de más frecuencia.

Podríamos formar un cuadro como el que sigue:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
25	37	48	54	43	97	65	24	38	47	51	93	48	71	81	43	97	38	51	58	41	21	17	03	01
19	50	11	29	18	13	15	34	23	27	28	82	80	70	41	14	26	02	07	08	09	05	13	22	98
				71			41				48								99			81		44
				31							06													

y sustituir las letras por los números de abajo. Este sistema de sustitución simple, a simple clave y múltiple representación, es seguro y casi indescifrable, que es cualidad primordial; pero tiene el inconveniente grave de la lentitud para cifrar y descifrar; y que la transmisión de tanto número por telégrafo se presta fácilmente a errores que complicarían todo mucho, e incluso alterar el criptograma.

Métodos de sustitución.-Diversos sistemas: Porta, Vigenère, Beaufort, Gronsfeld y de «regletas».

Un sistema de sustitución simple a simple clave puede ser—como hemos visto—de representación sencilla, doble o múltiple, teniendo esto por objeto, como no nos cansaremos de repetir, eliminar la frecuencia de las letras en el idioma.

Los sistemas a doble clave constan de una palabra Clave y un "Tablero de concordancia", que puede adoptar diferentes formas:

Sistemas a doble clave { 1.° Sistema a clave definida
2.° " " { indefinida o variable

1.° Son aquellos en que la clave que elegimos está compuesta por un número limitado e invariable de letras.

2.° Son aquellos en que el número de letras de la palabra clave varía.

Sistema Porta

En el siglo XVI se empleó el primer sistema de cifrar sustituyendo a doble clave; fué ideado por Porta; consistía en una tabla compuesta de 11 alfabetos recíprocos de 22 letras. A continuación la insertamos:

TABLA DE PORTA

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

De las 25 letras del alfabeto normal suprimimos las *J*, *K* y *U*. El semialfabeto de abajo se va decalando una letra cada vez.

Para cifrar por el Método Porta se toma una palabra que será la clave; por ejemplo, "metal", y se coloca debajo del mensaje a cifrar, si queremos que sea: *Necesito petróleo.*

Será:

Texto del mensaje: n e c e s i t o p e t r ó l e o
"Metal"— Tabla Porta } Clave: m e t a l m e t a l m e t a l m
Criptograma: f p s r l q i l c n a g l y n g

Debemos buscar el alfabeto en cuyo grupo de dos letras mayúsculas esté la letra de la clave (que está escrita debajo del mensaje) correspondiente a la de arriba que se desea cifrar.

De modo que en nuestro ejemplo, entramos en el grupo M N, y en cualquiera de los dos renglones buscamos donde esté la *n* (que deseo cifrar del texto) y la sustituyo por la que tiene encima (en este caso), que es la f, y así sucesivamente resultará el criptograma dicho.

Es un sistema de sustitución a doble clave (palabra y tabla) con alfabetos recíprocos con clave limitada.

Como vemos desaparece la frecuencia del idioma, al tomar para cifrar tantos alfabetos como letras no repetidas tiene la palabra clave. Tiene el inconveniente de que operamos con un número reducido de alfabetos y que necesita el empleo de ciertas palabras claves a fin de no reducir el número de representaciones.

En la época en que apareció este método de Porta hizo una revolución en el arte de cifrar, por lo que se llamó a su autor el padre de la Criptografía moderna.

Si deseamos emplear la "clave variable" podemos tomar las palabras M E - M E T - M E T A - M E T A L

M E - M E T - M E T A, etc., que tiene ventajas positivas, como fácilmente se comprende.

Mejorado el sistema Porta, apareció algunos años después Blaise Vigenere; presentó una tabla más perfecta que elimina las imperfecciones de la de Porta; a esa tabla más completa le llamó de "cifra cuadrada" o "cifra indescifrable", y aun está en vigor. La tabla consta de 26 alfabetos normales ordenados, decalándose una letra de uno a otro, lo mismo vertical que horizontalmente.

El uso de la tabla es muy sencillo. Se toma en la primera columna vertical izquierda la letra de la clave que corresponde a la del texto normal que deseamos cifrar, y esta letra (la que queremos cifrar) en el primer alfabeto horizontal de arriba y el punto de intersección de ambas coordenadas nos dará la letra cifrada. También se pueden buscar las letras inversamente, la de la clave en el horizontal y la del texto en el vertical. (Es cuestión de convenio.)

Si queremos cifrar:

Texto del mensaje = n e c e s i t o p e t r ó l e o

"Metal" } Clave = m e t a l m e t a l m e t a l m

Tabla Vg. }

resultará el criptograma = z i v e d u x h p p f v h l p a

Con el método Vigenere una letra cualquiera del texto del mensaje podrá estar representada por tantas otras letras distintas como letras diferentes tenga la palabra que tomamos por clave.

Como muestra de lo que se disminuye, con este método, la frecuencia del idioma pongamos el ejemplo siguiente:

Si hubiese una palabra de once letras iguales tal como: c c c c c c c c c c c, cifrándola por este método con una pala-

TABLA DE VIGENERE

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
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 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 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 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 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 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 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 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 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 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 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 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 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 p q r s t u v w x y z a b c d e f g h i j k l mn
P q r s t u v w x y z a b c d e f g h i j k l mn o
Q r s t u v w x y z a b c d e f g h i j k l mn o p
R s t u v w x y z a b c d e f g h i j k l mn o p q
S t u v w x y z a b c d e f g h i j k l mn o p q r
T u v w x y z a b c d e f g h i j k l mn o p q r s
U v w x y z a b c d e f g h i j k l mn o p q r s t
V w x y z a b c d e f g h i j k l mn o p q r s t u
W x y z a b c d e f g h i j k l mn o p q r s t u v
X y z a b c d e f g h i j k l mn o p q r s t u v w
Y z a b c d e f g h i j k l mn o p q r s t u v w x
Z a b c d e f g h i j k l mn o p q r s t u v w x y

En el alfabeto pone también la W; tiene, pues, 26 letras.

bra clave como MURCIELAGOS (1), de once letras diferentes, obtendríamos:

Texto: C C C C C C C C C C C
Clave: M U R C I E L A G O S
Criptograma: O W T E K G M C I Q U

ejemplo palpable de cómo desaparece la frecuencia.

El sistema Vigenere es, pues, a doble clave ("palabra" y "tabla") con alfabetos múltiples y normalmente ordenados. Es de doble sustitución porque el texto ordinario se sustituye por las letras de la clave y luego por las de la tabla.

Sistema Beaufort

El sistema Beaufort es análogo al Vigenere; utiliza su tabla, pero la busca de la letra sustitutiva es diferente. Toma en el alfabeto horizontal superior de arriba la letra correspondiente de la palabra clave, baja por esa columna hasta encontrar la letra del texto ordinario y corriéndose horizontalmente a la izquierda toma del alfabeto vertical primero izquierdo la letra cifrada.

Texto del mensaje = n e c e s i t o p e t r ó l e o
"Metal" / Tabla Vg. } Clave = m e t a l m e t a l m e t a l m
Criptograma = b a j e h w p v p t h n v l t c

Método Gronsfeld

El sistema Gronsfeld se basa en lo mismo que los anteriores de los alfabetos decalados. Tiene la ventaja que no se usa la tabla de Vigenere. Toma como clave un número

(1) Es raro, en nuestro idioma, encontrar una palabra donde entren las cinco vocales y no se repitan, ni éstas ni las consonantes.

cualquiera, que, como todas las claves, se escribe debajo del mensaje corriente o texto ordinario y cada número indica el avance que hay que dar a la letra que nos ocupa para obtener la sustitutiva que la cifra. Esto es, indica el decalaje que tenemos que dar al alfabeto normal para obtener aquel en que hemos de cifrar. Ejemplo:

Escribamos el abecedario normal

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
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

Texto: n e c e s i t o p e t r ó l e o

Número y sistema 7531 Clave: 7 5 3 1 7 5 3 1 7 5 3 1 7 5 3 1

Criptograma: u j f f z n w p w j w s v q h p

De modo que es como si hubiésemos cifrado con el Método de Vigenere y con la clave: 7 5 3 1 = H F D B

El sistema Gronsfeld se usa más que el de Vigenere por la facilidad con que mentalmente se hace el cifrado y descifrado. Tiene el inconveniente de que requiere claves cortas para recordar los números de memoria. Se recomienda, por ser más fácil para retener en la memoria, usar la palabra y a cada letra darle, por ejemplo, el valor del número que indique su lugar en el abecedario normal.

En los sistemas estudiados de Porta, Vigenere, Beaufort y Gronsfeld cuando se emplean claves cortas presentan ciertos defectos que los criptólogos aprovechan para descifrarlos furtivamente.

El método de "regletas" es una modificación de la tabla de Vigenere; consiste en una regla plana ancha, dentro de la cual se desliza por su centro otra regleta de doble longitud. En la primera se escribe el alfabeto normal y en la que corre se escriben dos alfabetos normales, uno a continuación de otro. Al correrse la regleta se comprende que

se decalan los alfabetos lo que se desee. Puede no estar el alfabeto de la primera regla ordenado normalmente, pero en ese caso, los dos que se escriben seguidos en la regleta central han de estar ordenados como el primero.

Esto, para facilitar la inteligencia entre los corresponsales; pero los alfabetos pueden estar escritos de cualquier modo, ahora que en este caso, habrá que enviar al corresponsal copia literal, exacta, de las regletas. (Cuestión de convenio.)

Con ellas es fácil cifrar y descifrar.

Método de sustitución. – Método llamado de «los militares». – Métodos para disminuir la «frecuencia».

El sistema llamado de los militares consiste en una tablilla y una cinta que corre; analicemos su empleo.

Se escribe el alfabeto ordinario normalmente ordenado y se pega en una tablilla; debajo de este alfabeto corre una cifra sin fin con dos alfabetos escritos, uno a continuación de otro. Los alfabetos que se escriben en esta cinta pueden ser alfabetos intervertidos. La separación de letras serán iguales en todos ellos. Debajo de las letras del primer alfabeto fijo en la tablilla se ponen ocho casillas verticales para repartir bien los números y en estas casillas se escriben donde y como se quiera los 90 números de dos cifras, del 10 al 99, dejando entre uno y otro los huecos que bien nos parezcan. Con objeto de que cada letra tenga debajo un número aproximado de grupos de cifras, llenaremos solamente tres o cuatro huecos de los ocho que existen. Para facilidad y evitar confusiones se escribirán los números correlativamente, como indica la tabla.

La cinta de que hablamos se mete por los dos extremos a y b.

El alfabeto se escribe tomando una clave, por ejemplo, la palabra *navío*.

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

	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					

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

tomando el alfabeto en diagonal sería:

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

Para cifrar se indica qué letras de los dos alfabetos, superior e inferior, coinciden: A = R

Texto a cifrar: *Deseo evacuar heridos.*

d e s e o e v a c u a r h e r i d o s
16 66 46 42 25 91 37 61 23 30 86 70 50 98 31 15 64 77 20

Ventajas: Que una vez hecha la tablilla (o teniéndola) es fácil hacer el cifrado.

Inconvenientes: Que duplica los guarismos y, por tanto, es lento para cifrar y descifrar y resulta caro para transmitir. No tiene puntuación (es fácil de remediar) y eso hace que pueda resultar confuso, y, principalmente, como una vez elegida la clave todo es fijo, resulta que puede descifrarse.

Métodos para disminuir la frecuencia del idioma.

Para evitar la frecuencia del idioma, ideal que debe perseguir todo criptógrafo, se pensó hacer una tabla donde el tamaño del área que representa cada letra sea proporcional a la frecuencia o repetición de esa letra en el idioma. De este modo no cabe duda que se disminuirá notablemente la repetición de la letra en el criptograma.

Clave 12105.

	4	7	9	0	5	3	1	6	8	2
0										
9			A			E			I	
2										
5				O		U			N	
4										
3			S			R			L	
7										
1		C		D		T	M	P	b	f
8									g	h
6	j	k	ñ	qu	v	w	x	y	z	Paso

4	7	9	0	5	3	1	6	8	2
.	,	;	:	....	¿?	¡!	[ ]	“ „	
◤	◥	◡	—	Die-resis	Ce-dilla	Apos-trofo			
æ	œ								
ü									
güe	güi								
1	2	3	4	5	6	7	8	9	0
Conv.º 1º	Conv.º 2º	Conv.º 3º	Conv.º 4º	Conv.º 5º	Conv.º 6º	Conv.º 7º	Conv.º 8º	Conv.º 9º	Conv.º 10º
							Paso	Cambio de clave.	
									&

En cada mil letras entran la:

E	A	O	S	N	R	I	L	D	U
133	126	93	78	68	64	63	55	50	43

que son las 10 letras que más se repiten.

Con arreglo a esos tantos por mil se forma la tabla de la página anterior:

Cada letra está representada por las dos cifras cuyas coordenadas se cortan en el área en que está escrita. De modo que la *A* tiene las 12 representaciones siguientes:

04 07 09 00 94 97 99 90 24 27 29 20

La E tiene ..... 12 representaciones.
O 10
S 8
I, N, R, L. 6
U, C, D, T. 4
M, P. 2
B, F, G, H, J, K, Ñ. Qu. V, X, Y, Z..... 1

Pongamos un ejemplo:

Texto a cifrar: Tengo 21 heridos.

Clave: L o c o r t é s n o (qu) i t a l o v a l i e n t e.–12105
6 8 1 7 3 4 5 2 9 0 4 7 9 0 5 3 1 6 8 2

Con la clave se ponen los números de la periferia de la tabla.

Texto = T e n g o 2 1 h e r i d o s
Criptograma = 15 91 46 88 50 62 37 34 62 82 96 73 22 10 45 30

Se dará para el telégrafo en esta forma:

12105—15914—68850—62373—46282—96732—21045—30

(se completan las cinco cifras con números a capricho).

Este ingenioso método es muy difícil de descifrar.

Métodos de sustitución.—Sistema de «clavijas».—Sistemas de Bigramas.—Tablas de cifrar y descifrar.—Criptógrafos de bigramas.—Forma triangular.

El tablero tiene la forma que indica la figura. En las 10 casillas primeras verticales y horizontales se ponen los números de la clave como en los métodos ya estudiados. En la primera línea horizontal se ponen las clavijas que tienen las 10 letras que más se repiten en el idioma. (Letras móviles.)

E A O S N R I L D U

y en el cuadrado indicado con trazo más grueso, abajo a la derecha se escriben las letras que faltan del alfabeto normal escrito por su orden corriente; además se ponen los signos de puntuación, etc., que indica la figura.

Cada vez que criptografiamos una letra movible la quitamos de su casilla y la llevamos a la primera casilla que se halle vacía (de izquierda a derecha), desde donde surgirá su efecto la próxima vez que tengamos que criptografiarla de nuevo y así sucesivamente, sin retroceder nunca; de este modo si el criptograma es largo y, por tanto, se repiten muchas letras, recorreremos con las clavijas todas las casillas desde la 94, que es la primera vacía, al empezar el criptograma, hasta la 69, que es la última de todas, y entonces comenzaremos de nuevo poniendo la clavija en la primera que *ahora* se encuentra vacía, que será la 04.

Clave 12105.

	④	⑦	⑨	⓪	⑤	③	①	⑥	⑧	②
⓪	E	A	O	S	N	R	I	L	D	U
⑨	o	o	o	o	o	o	o	o	o	o
②	o	o	o	o	o	o	o	o	o	o
⑤	o	o	o	b	c	ch	f	g	h	j
④	o	o	o	k	ll	m	ñ	p	qu	rr
③	o	o	o	t	ü	v	w	x	y	z
⑦	o	o	o	güe	güi	æ	œ	.	,	;
①	o	o	o	:	.....	¿?	¡!	( )	"„	'
⑧	o	o	o	Apostrofo	Diéresis	Cedilla	1	2	3	4
⑥	o	o	o	5	6	7	8	9	0	Cambio de clave.

Nos lo explicaremos mejor poniendo un ejemplo:

Texto a cifrar: Tengo 21 heridos leves.

Clave: Lo cortés no quita lo valiente.—12105.

L o c o r t é s n o (qu) i t a l o v a l i e n t e
6 8 1 7 3 4 5 2 9 0 4 7 9 0 5 3 1 6 8 2

Texto= t e n g o 2 1 h e r i d o s l e v e s
30 04 05 56 09 86 81 58 94 03 01 08 99 00 06 90 33 24 98

Este método es molesto por tener que llevar la tabla, pero es bastante indescifrable.

SISTEMA DE BIGRAMAS

Si consideramos las 26 letras del alfabeto con que venimos trabajando podremos hacer con ellas 26 × 26 = 676 grupos de dos letras o bigramas, y por tanto, pueden ser representados por números de tres cifras; como tenemos 999 — 100 = 899, es decir, 899 números de tres cifras y solamente existen 676 bigramas, no hay duda de que nos sobran números para las representaciones que necesitemos.

Como en los métodos últimamente explicados *cada letra* la representamos por números de *dos* cifras (coordena y abscisa), para representar cada bigrama necesitaríamos cuatro guarismos y como con este sistema de bigramas nos basta, para representar un grupo de dos letras, con tres guarismos; nos ahorramos por cada bigrama un guarismo, esto es, un 25 por 100.

Ahora bien, el procedimiento más sencillo que se ocurre para cifrar los bigramas sería hacer un código o tabla en que coloquemos los 676 bigramas por orden alfabético y a cada uno de ellos ponerle al lado un número cualquiera de *tres* guarismos, pero teniendo cuidado de que no se repitan los números. Esta sería la tabla para cifrar.

Para formar la tabla con que descifrar pondríamos esos números en columnas por orden correlativo y al lado los bigramas que representaban y así, como ocurre con las claves silábicas, tendríamos el código completo de bigramas.

Para facilitar el cifrado y disminuir su frecuencia en el idioma (que también existe, aunque en menor escala) podemos hacer cuadros especiales o tablas en que figure cada bigrama representado por un área proporcional al número de veces que se repite en el idioma, como indicamos al hablar de las letras. Al poner los bigramas en estas tablas, los representaríamos por coordenada y abscisa y el tercer

guarismo indicaría el número de la tabla en que se encontraba; es como si dijéramos la tercera dimensión. (Ver criptógrafo de bigramas número 8.)

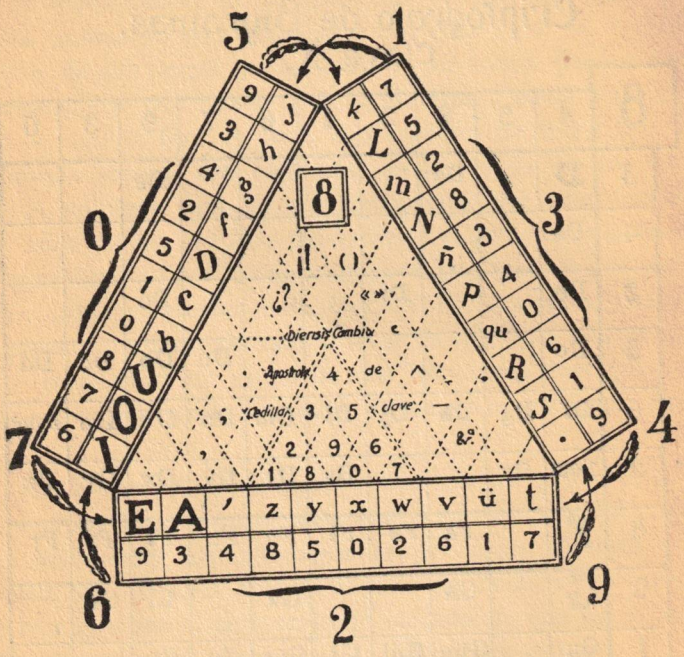
Criptografo de Bigramas.
Clave X.

8	4	5	8	2	1	6	7	9	3	0
3	D		Da					De		
4	De									
2	De			Di				Do		
5	Do						Du	Db	Dc	Dd
6	Df	Dg	Dh	Dj	Dl	Dm	Dn	Dñ	Dp	Dque
9	Dqui	Dr			Ds	Dt	Dv	Dx	Dy	Dz
8	F		Fa	Fe	Fi	Fo	Fu	Fl	Fr	Ft
0	G		Ga			Ge		Gi	Go	
1	Gu		Güe	Güi	Gl	Gm	Gn	Gr		
7	H		Ha			He	Hi	Ho		Hu

El principal inconveniente que tiene este método es que requiere mucha superficie el código y la falta de agrupación e imposibilidad de escribir algunas palabras con bigramas que, aunque se puede salvar la dificultad, no resulta muy práctico.

Es muy buen método, pues casi es imposible de descifrar sus claves, si imprimimos diez claves y se cambian con un orden convenido, resulta imposible "casi" de descifrar.

Forma triangular.
Clave 12107.



Letras que conviene lleven las mismas cifras.

E	j	.	x	b	qu
A	h	ñ	w	f	m
'	g	p	v	I	R
z	U	N	ü	c	S
y	D	L	t	O	k

Forma triangular. (Ver figura.)

Ejemplo:

Enemigo huye con 12 heridos.

En em ig oh uy ec on 1 2 he ri do s
998 992 064 073 785 691 578 808 818 739 166 057 319

El primer número de los tres que designan el bigrama indica el sector donde están las letras. Cuando las dos no están en un mismo lado, entonces el primer número indica el de la flecha que une los dos sectores donde hemos de buscar las letras.

Los números, puntuación y otros signos o convenios están en el centro, número 8. Para criptografiar un número, se escribe primero el 8, como hemos dicho, y luego, a continuación, los dos siguientes que marcan las coordenadas que lo indican (siempre de los dos sectores de arriba), primero, las decenas—sector n.° 0, de la izquierda—y luego las unidades—en el sector n.° 3 de la derecha—y los números de de arriba indican las coordenadas, que nos designan los que deseamos.

Este método no es de uso frecuente.

Método de sustitución octogonal y diagonal.

Otra tabla fácil de formar consiste en escribir los alfabetos en línea horizontal y vertical y en las 676 cuadrículas poner diferentes bigramas, que servirían para cifrar los mensajes ordinarios, entrando en la tabla análogamente a como lo hicimos en la tabla de Vigenere.

Este sistema no quitaría la frecuencia del idioma, y las letras repetidas estarían ahora denunciadas por los grupos de dos letras, el bigrama, que se repetiría tantas veces como aquella letra.

Para evitar la facilidad de un descifrado furtivo sustituímos directamente los bigramas del texto; suele dividirse el texto claro en cuatro pedazos, por ejemplo, y alternándolos ponemos de dos en dos uno encima de otro y ciframos los bigramas verticalmente. Ejemplo:

Texto: Enemigo huye desmoralizado, conviene perseguirlo.

Lo colocaríamos como sigue:

$$\begin{matrix} 4 & & 3 \\ \text{erseguirle} & & \text{doconvienep} \\ \text{desmoraliza} & W & \text{enemigohuye} \\ 2 & & 1 \end{matrix}$$

y se toman los bigramas ed - re - ss - em... y con ellos se entrará en la tabla de bigramas. Los que obtengamos se colocarán horizontalmente y los dividiremos en grupos de cinco letras. No conociendo la tabla de bigramas este método es casi indescifrable.

El representar los bigramas por tres números es lo más corriente, pues se presta a muchas más modificaciones que

si los representamos por 2, pues aparecería más pronto la frecuencia del idioma, que hay que evitar a todo trance.

Otro método ingenioso es el llamado de sustitución ortogonal y diagonal. Con una palabra clave y el alfabeto se forma la tabla. Sea la palabra clave "metal" y la tabla:

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

Si nosotros aceptamos una convención cualquiera cifraremos fácilmente los bigramas. Supongamos la palabra a cifrar dividida en grupos de dos letras y busquemos éstas en la tabla. Pueden ocurrir tres casos:

1.° Que las letras estén en una misma línea horizontal; en este caso las sustituímos por las dos que estén debajo.

2.° Que estén en una misma línea vertical; y se reemplazan por las dos que están a la izquierda.

3.° Que estén en renglones diferentes, sin coincidencias, y entonces se sustituyen por sus letras de arriba o de abajo que forman cuadro. Por ejemplo:

Texto a cifrar: T e l e g r á f i c a m e n t e
Criptograma: d c g c s f t d h b f b i l d c

Es conveniente también, usando este método, descomponer el texto claro en varias partes (dos, al menos), y colocarlas una sobre otra para cifrar los bigramas verticales que vayan resultando. Así no hay denuncia probable de la frecuencia del idioma.

Se puede, asimismo, para cifrar, tomar las diagonales en lugar de las correspondientes verticales y horizontales que hemos considerado. Es cuestión de convenio.

Diversas claves. — Autoclave.— Clave interrumpida.—Métodos de trasposición o perturbación.

Hemos visto los principales métodos de cifrar los mensajes, y al estudiarlos hemos empleado diferentes claves. Pero en éstas aun cabe más variación de las que hasta ahora hemos hablado. Ni que decir tiene que la clave variable da mucha seguridad al cifrado. En la milicia, en casos concretos en que se espera una orden corta y determinada, suele emplearse para cifrar la "auto-clave"; como su nombre indica, tomamos por clave el mismo mensaje que deseamos cifrar, y lo decalamos, por ejemplo (usando la tabla Viguenére):

Texto=	A v a n z a r r e s u e l t a m e n t e
Clave=	e a v a n z a r r e s u e l t a m e n t
Criptograma=	e v v n m z r i v w m y p e t m q r g x

Este sistema requiere como condición indispensable conocer lo que nos van a decir, lo que limita muchísimo su empleo; pero en momentos decisivos puede ser muy eficaz, pues como se empleará poco, con frases cortas y mezclado con otros criptogramas cifrados por otros métodos, es muy seguro y será muy difícil que el enemigo pueda descifrarlo.

Tiene el grave inconveniente de que si llegara a suprinirse una letra en la transmisión telegráfica sería así indescifrable, por lo menos se tardaría muchísimo.

La llamada clave interrumpida es aquella que se la corta a voluntad por medio de una letra muda que intercalamos donde lo deseemos.

Por ejemplo:

Texto=N	e	c	e	s	i	t	o	p	e	t	r	ó	l	e	o						
Clave=m	e	t	w	a	w	l	m	e	t	a	l	w	m	w	e	t	a	l	m		
Criptograma=z	i	v	w	e	w	d	u	x	h	p	p	w	f	w	v	h	l	p	a		

En este sistema a clave interrumpida, como el anterior de autoclave, lo que se pretende con ellos es dificultar lo que se llama el "factoreo", que es uno de los procedimientos principales para descifrar los criptogramas furtivamente.

Métodos de trasposición o perturbación.

En estos métodos—como sabemos—no se emplean letras nuevas, solo las del mensaje mezcladas o traspuestas. La clave da el orden en que debe efectuarse la trasposición. La clave puede ser simple o doble.

El primer sistema de trasposición conocido se debe a los griegos. En un palo ligeramente tronco-cónico envolvían una tira de papel (especie de serpentina), cubriéndolo helicoidalmente. El mensaje se escribía en claro a lo largo de una generatriz. Luego se desenvolvía del palo y se enviaba la tira a quien fuese; éste al recibirla la enrollaba en un palo análogo y una vez hecho, girándolo, encontraba en una de las generatrices el texto claro.

En el siglo XVI se empleó con éxito un sistema llamado de "rejas", también se llamó de rejilla o grilla. Consistía en una tabla de madera, metal o cartón donde se practicaban a voluntad unas ventanitas en tamaño de las letras. Se ponía la tabla sobre un papel de su tamaño, y por aquellos huecos se escribía el mensaje en claro; se levantaba la tabla y se rellenaba el papel con otras letras a capricho. Estas aberturas podían seguir dibujos más o menos fantásticos.

Para descifrar era necesario otra tabla idéntica. Es el sistema más difícil de descifrar furtivamente.

Hoy no se usa por lo poco práctico de la clave.

Método Universal de trasposición o perturbación.

Texto a cifrar: Oh la fábula de España; Gravina, al contrario es todo genio y decisión en el combate, los españoles se han batido como leones (1).

Clave: Lo cortés no quita lo valiente.—12105 (2).

1				2
L	O	C	O	R
T	E	S	N	O
Q	U	I	T	A
L	O	V	A	L
I	E	N	T	E
3				4

R T E S N O Q U I T - A L O V A L I E N T
5 7 0 6 2 3 4 9 1 8 - 0 4 7 9 1 5 3 2 6 8

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

(1) De una carta de Napoleón a Decrés.

(2) En este ejemplo, consideramos a la *q* y la *u* por separado.

Texto seguido a intervalo de 10 letras:

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

CRIPTOGRAMA

E B I O H A N A T D - D P A R E A S E Ñ G
C L N S O E O M O E - D N Y E O I E G O D
T I S O R O R A E T - A A C N V A N I L O
C A L S O T B M E O - O F U A H A A L B L
E Ñ E S S O A P L S - C O N L I N I S E E

Terminaremos esta parte de cifrar, poniendo ejemplos sencillos (sin llevar encima clave material) de trasposición simple, para ensayar en ellos más adelante el "factoreo".

Supongamos que deseamos cifrar:

"Necesito agua y carbón para poder navegar", y sea la clave "metal". Escribimos el texto en grupos de 5 letras (las de la clave) unos debajo de otros, y sobre esos grupos

4	2	5	1	3
n	e	c	e	s
i	t	o	a	g
u	a	y	c	a
r	b	o	n	p
a	r	a	p	o
d	e	r	n	a
v	e	g	a	r

escribimos los números que indican las letras de la palabra clave:

m e t a l, numeremos las letras, según aparece en el alfabeto, y será: 4 2 5 1 3,

4 2 5 1 3

y ahora, tomando las columnas verticales en un orden convenido, resultará el criptograma, por ejemplo:

1 2 3 4 5 será: eacnp-naeta-brees-gapoa-rniur-advco-yoarg

Es un caso de simple transposición a columnas completas.

Este método de cifrar a cuadro o columnas completas así simplemente, limita mucho su empleo y tiene fácil tanteo para descifrar; se busca un divisor del número total de letras, y ese número será el de letras de la clave; si escribimos las letras del criptograma en tiras de papel, y las vamos poniendo unas al lado de otras; las tanteamos, hasta que salga claro, y lograremos descifrar el criptograma. Para evitar esto empleamos una clave que no tenga el número de letras divisor del total del texto, y completamos las que falten con letras mudas, bien al final o bien intercaladas en el texto, en sitio donde no pueda haber confusión ninguna.

Ni que decir tiene que las columnas verticales pueden cogerse de arriba a abajo unas (las impares, por ejemplo), y las pares, de abajo a arriba, o haciendo otra cualquiera de las muchas combinaciones que fácilmente se ocurren.

Si nosotros, el criptograma anterior lo sometemos a un nuevo cifrado con otra palabra clave, para que no quede a columnas completas, será, por ejemplo: sea la clave:

e s l o r a
2 6 3 4 5 1

2 6 3 4 5 1
e a c n p n
a e t a b r
e e s g a p
o a r n i u
r a d v c o
y o a r g w

y de aquí sacamos el criptograma deseado.

n r p u o-w e a e o-r y c t s-r d a n a-g n v r p-b a i c g-a e e a-o w w w w

El criptoanálisis de los cifrados a doble transposición se basa en la palabra probable.

En la milicia lo esencial es que *no se descifren pronto* los mensajes urgentes, pues si logramos que tarden más de uno o dos días, ya no tendrá actualidad y no tendrá eficacia el conocimiento de su contenido.

Criptógrafos de «regletas» y «discos».-Aparatos Bazaries y Soudart. Máquinas de cifrar.

En los últimos cincuenta años, la criptografía, como todo, avanzó rápidamente, y puesto que para cifrar hace falta una clave y un sistema constante aplicado a ella, se pensó lógicamente que tales cosas podían efectuarse mecánicamente.

Las máquinas calculadoras, de mil sistemas diferentes, y las máquinas de escribir, al perfeccionarse en su mecánica, dieron casi resuelto el problema que nos ocupa.

Los dos sistemas mecánicos que se han ensayado de "regletas" y de "discos" obtuvieron prontamente gran perfeccionamiento.

El sistema de "regletas", aunque daba fácilmente sustituciones dobles con alfabetos incoherentes, más o menos regularmente ordenados, se desechó casi en absoluto, o, por lo menos, adquirieron gran predominio sobre él los sitemas a base de discos, por las facilidades mecánicas que presentaba su construcción.

El sistema de discos concéntricos con alfabetos en su periferia, nos proporciona fácilmente el sistema de sustitución con alfabetos ordenados o incoherentes. Los discos triples, cuádruples, múltiples, son también sustituciones.

Los discos más empleados son los que llevan las letras en su canto.

El 1891, el Capitán Bazaries inventó un aparato muy interesante para cifrar. Se compone de 20 discos de igual diámetro, montados sobre un eje central, en forma de que puedan girar. Los discos están numerados del 1 al 20.

Cada uno de estos discos tiene en el canto de su periferia un alfabeto incoherente. Los discos, naturalmente, pueden montarse en el eje según un orden cualquiera, y giran libremente; por medio de unas muescas pueden quedar aprisionados.

El aspecto exterior del aparato es análogo a los candados de letras. Veamos su funcionamiento.

Para montar los discos en el eje que le sirve de alma tomamos una frase cualquiera de veinte letras (número de los discos); a esta frase damos números a sus letras, como hicimos otras veces con las claves, no repitiendo los números en letras iguales, sino continuándolos; sea la frase:

L A M A R I N A E S I N V E N C I B L E
12-1 - 14-2-18-9-15-3 - 6-19-10-16-20-7-17-5-11-4-13-8

y metemos los discos numerados por el orden que indica la clave, y cerramos el eje por sus extremos.

Para cifrar un mensaje cualquiera dividiremos su texto en grupos de veinte letras, y girando los discos convenientemente escribiremos en una generatriz del cilindro las palabras del texto claro, y en las veinticinco generatrices restantes del cilindro tendremos otros tantos criptogramas diferentes, que nos representarán el mensaje deseado.

El que reciba el criptograma montará los discos de su aparato según la clave; una vez colocados así, escribirá girando los discos, en una de las generatrices, las letras del criptograma recibido por el orden que vengan, y girando el cilindro-aparato verá en otra generatriz el texto claro.

Este sistema es de sustitución doble con alfabetos incoherentes a múltiple representación.

El número de permutaciones que pueden hacerse con los discos es de dos quintillones.

Parece que el criptograma así obtenido ha de ser indescifrable, pero no fué así; el Marqués de Viaris, en 1893,

ensayando un sistema basado en la "palabra probable" y en el hecho de que una letra del texto ordinario no aparece representada en el criptograma más que por doce o trece letras en una generatriz cualquiera, le permitió descifrar un gran número de cifrados hechos con estos discos.

El año de la guerra, el 1914, Soudart introdujo grandes perfeccionamientos en el aparato Bazaries, variando la colocación de los discos y, con cierto ritmo, el giro de los mismos, obteniéndose así doble transposición, lo que ha hecho que los criptogramas de ese aparato sean prácticamente indescifrables.

Perfeccionando aún más esos aparatos se ha llegado a las máquinas de cifrar modernas, parecidas a las corrientes de escribir. Tienen un teclado donde escribimos el texto ordinario, y va saliendo en la cinta el criptograma correspondiente. El interior de la máquina está formado por discos giratorios, que de un modo ingeniosísimo, con palancas, muescas y camones, cambian la situación y giran o se detienen convenientemente. Están numerados, como es lógico suponer.

Para descifrar, el que recibe el criptograma, que posee una máquina igual, no tiene más que colocar los discos según la clave convenida, y una vez hecho esto, escribir en su teclado el criptograma tal y como lo recibe, y en la cinta va saliendo el texto claro.

De este modo se cifra en general, mediante sustitución a doble clave con alfabetos incoherentes, o bien sustitución y transposición, que hacen que salgan los criptogramas casi indescifrables, esto es, prácticamente indescifrables.

Las naciones que más se han especializado en esto han sido Alemania, Holanda, Francia y Estados Unidos, llegando a obtener verdaderas maravillas.

En los modernos Gabinetes de Criptografía, las máquinas de cifrar están montadas con todo lujo de detalles para

el secreto; metidos en cámaras acorazadas, las manejan desde allí los Oficiales del E. M., y por conexiones eléctricas transmiten sus signos criptografiados, fuera de estas cámaras secretas (rojas o negras, así se llamaban en algunos países durante la Gran Guerra) para su transmisión.

También existen unas máquinas de cifrar, muy pequeñas, cuyo aspecto exterior, es un reloj de bolsillo. Son muy ingeniosas y de fácil manejo.

Criptoanálisis furtivos.–Sistemas de «factoreo» y de «la palabra probable».

Criptoanálisis furtivo.—Se llama así—como sabemos—el arte de poner en claro los criptogramas que sorprendemos, sin conocer, naturalmente, la clave.

En líneas generales, diremos que todos los métodos estudiados para descifrar están basados en la ley de "frecuencia" del idioma.

Para descifrar criptogramas de sustitución a doble clave con alfabetos regularmente ordenados, como los métodos Porta, Vigénere, Beaufort y Gronsfeld, inventó Kasiski un método que llamó de "análisis por factoreo". En todo método a doble clave hay que buscar dos incógnitas: el número de alfabetos empleados, que será el de letras diferentes de la clave, y el orden en que estén colocados esos alfabetos, que nos llevará al conocimiento de la tabla.

En la simple enunciación de las dos conclusiones anteriores ya vemos que cuanto más larga sea la clave, más se dificulta el descifrado furtivo del criptograma.

Los criptogramas largos serán más fáciles de descifrar furtivamente que los cortos; pues en éstos tal vez no haya lugar a ver con claridad las repeticiones que denuncien la frecuencia del idioma.

En los criptogramas largos, dos grupos de polígramas semejantes, son producidos por dos grupos de letras semejantes del texto claro, que han sido cifrados con los mismos alfabetos.

El número de letras que haya entre dos grupos semejan-

tes será el número de letras que tiene la clave, y conocido esto se conocerá el número de alfabetos utilizados. Sabido lo anterior, sólo nos queda para conocer la clave completa, saber el orden de colocación de los alfabetos utilizados.

Para averiguar esto, dividiremos el texto cifrado en grupos de letras numéricamente igual al de la clave que presumimos, y los colocaremos unos encima de otros. De esta forma, cada columna o fila vertical de letras corresponderá a un mismo alfabeto (puesto que lo determina la clave), y sólo nos quedará, por tanto, aplicar la tabla de frecuencia del idioma a cada columna.

La letra que más se repita en esa columna será la correspondiente a la "E" del texto claro, y buscando en la tabla de Vigénere en cuál de sus alfabetos viene la "E" representada por la letra que en la columna que nos ocupa se repite más, podremos descubrir la clave.

Claro que no todo es tan sencillo como lo hemos expuesto. Tendremos que hacer muchísimas intentonas, y sólo a fuerza de aproximaciones sucesivas iremos descubriendo las incógnitas, pues ni los grupos de letras semejantes, indicadoras del número de letras de la clave, será claro y terminante desde el primer momento, ni las letras de la columna se repetirán en forma que indiscutiblemente nos diga cuál es la representación de la "E" en ese criptograma. Pero, repetimos, personas hábiles y entrenadas hallarán en los métodos expuestos un procedimiento a investigar y llegar al conocimiento de lo deseado.

El procedimiento apuntado sólo tiene aplicación en criptogramas hallados por los métodos en que empleemos alfabetos ordenados, como los de la tabla de Vigénere. Si para cifrar usamos de alfabetos incoherentes, entonces el sistema de factoreo no dará resultado ninguno.

El Capitán Bazeries, inventor del criptógrafo de discos, ensayó con éxito el método de "la palabra probable", que

puede aplicarse con buen resultado a criptogramas cifrados con alfabetos ordenados o incoherentes.

Cuando presumimos que en un criptograma, por las circunstancias que rodean el momento de la emisión, debe haber una palabra determinada, cifrada, como División, o el nombre de un buque, de un Almirante, de una acción, si como es lógico existe, ya tenemos algo para darle vueltas y hacer luz en ese asunto. Estos indicios u otros, proporcionados por el espionaje, o como sea, nos darán luces para conseguir el fin perseguido.

Los criptogramas comerciales son los más fáciles de descifrar; si se citan cantidades numéricas altas, por ejemplo, treinta mil, luego vendrán los cientos, y las decenas, y las unidades, etc. Los nombres de los géneros a tratar, según la población productora y la casa que lo pide o lo manda, etcétera, son datos muy preciosos y utilísimos. En la parte militar se ingeniarán más para hacer el "despiste". En el comercio, los códigos para cifrar tienden a tener frases hechas, a representar con pocos guarismos muchas cosas; la economía es el móvil principal de esta Criptografía.

"La palabra probable" la colocamos debajo de las primeras letras del cifrado y trabajamos con los cuadros y sistemas conocidos, operando con ellos (como si fuese la clave); si con lo que obtengamos, estudiado minuciosamente, no vemos ninguna palabra clara que nos indique cuál puede ser la clave, correremos la palabra probable un lugar a la derecha, y volveremos a trabajar con los cuadros dichos. Y así sucesivamente hasta obtener la clave.

Para descifrar el criptograma, si hubiésemos empleado alfabetos incoherentes, tendríamos que conocer la tabla que hubiésemos empleado, y entonces, practicando un procedimiento análogo, hallaríamos la clave.

La sustitución a doble clave con alfabetos incoherentes es prácticamente indescifrable.

La clave variable impide aplicar con éxito el factoreo. La

variación debe ser irregular (señalada por la letra muda), pues si la variación es regular, al fin y al cabo se indicará ésta, y será una probabilidad más a favor del descifrado furtivo. El uso de alfabetos incoherentes con clave variable llena las necesidades corrientes militares.

La sustitución a doble clave indefinida es muy recomendable; la clave indefinida suele ser la página de un libro cualquiera, que puede variarse los días pares, por ejemplo. Generalmente, estos libros son códigos a propósito para cifrar.

Códigos para cifrar.—Trigramas. Tetragramas etc.—Sistemas mixtos de bigramas y trigramas.—Claves silábicas.—Ventajas e inconvenientes de cifrados con códigos u otros procedimientos.—Normas a tener en cuenta para cualquier cifrado.

Antes de entrar en los Códigos hablemos ligeramente sobre trigramas, tetragramas (cuatro letras), etc., y métodos mixtos de bigramas y trigramas.

Los trigramas formados con las 26 letras son $26^3 = 17.576$; necesitamos, por tanto, grupos de 5 cifras para representarlos, y tendríamos una pérdida, por tanto de 8 % respecto a los bigramas.

En el idioma español los trigramas usuales pueden reducirse a 10.000, y, por tanto, representarlos por grupos de 4 cifras, con lo que obtendríamos un beneficio de 8,5 % en lugar de la pérdida antes aludida. Los trigramas no son prácticos a nuestros usos.

Los tetragramas (4 letras), pentagramas (5 letras), etc., no se usan por las complicaciones que introducen tantas cifras para representarlos, pero los mencionamos porque pueden servir, y sirven, para la formación de los Códigos.

Hasta ahora hemos representado por el mismo número de cifras a grupos iguales de letras; y si nos fijamos que en la práctica esos grupos de letras se repiten con mucha desigualdad, comprenderemos que estudiando esto podemos obtener una economía al hacer los criptogramas, si representamos cada grupo de acuerdo con la frecuencia que se usa.

Veamos la economía que se emplea usando un método mixto de monogramas y bigramas.

Si con los 100 números de dos cifras empleamos 26 en representar las letras del alfabeto, quedan 74, que podemos asignar a otros tantos bigramas, con lo que aproximadamente, tendremos en 100 letras 75 expresadas por una cifra, puesto que serán grupos de dos letras expresados cada uno por dos cifras y 25 letras sueltas representadas cada una por dos cifras. Esto es: 100 letras y 125 cifras, lo que comparado con el método llamado de los militares nos da un ahorro del 37 por 100.

Hay tablas mixtas de monogramas y bigramas que facilitan mucho todo esto, pero como no se usan en la Criptografía militar moderna, no insistimos sobre ello; bástenos con decir que si consideramos 5 cifras que constituyen una palabra telegráfica, resulta, por el método que explicamos llamado de los militares 2 1/2 letras; por el método de bigramas 3 1/3 letras, y por el método mixto que ahora tratamos ligeramente 4 letras.

Cifrando una frase cualquiera por los tres métodos, comprobaremos cuanto decimos.

Si hacemos un estudio comparativo análogo entre bigramas y trigramas, como en castellano los bigramas son menos de 500 (incluyendo letras sueltas y signos), podemos aprovechar los otros 500 para los trigramas más frecuentes.

De este modo cada trigrama que se encuentre resulta representado por tres cifras (a letra por cifra), y cada bigrama tres cifras (a 2/3 de letra por cifra); resultando del cálculo práctico verificado en algunos miles de letras que nos da este método, por 5 cifras 4,25 letras. Estudiando el ahorro que nos proporciona, resulta un 41,5 por 100 respecto al método corriente llamado de los militares. (Núñez.)

Y así sucesivamente.

Claves silábicas.

Constan de dos partes, una para cifrar y otra para descifrar.

En la primera van impresas por orden alfabético las sílabas del castellano, y a su derecha se escriben en un orden cualquiera los mil números de 3 cifras, desde el 000 al 999.

En la segunda parte van impresos los números por orden correlativo, y a su derecha las sílabas correspondientes a la clave cifrada.

Para reducir a mil las sílabas en nuestro idioma, se han deshecho los diptongos y triptongos y aunque en el español hay más de 1.000 sílabas, si sólo consideramos las más corrientes puede muy bien hablarse con las que se han tomado.

Los inconvenientes de esta clave son:

1.° Ser doble, lo que se evitaría dándoles la forma de cuadrados.

2.° El mucho tiempo que se emplea para preparar una clave. Puede calcularse en 6 horas. (Según el criptógrafo Núñez se puede llegar a hacer en muchísimo menos tiempo.)

3.° Para la extensión de la clave, dá poca economía en las transmisiones telegráficas. El criptógrafo Carmona dice que a 3 cifras corresponden 2,30 letras, o sea a 5 cifras 3,83 letras; pero Núñez ha calculado 25.000 sílabas y no alcanza más que a 3,66.

4.° Mucha superficie (medio metro cuadrado aproximadamente) que cansa y marea cuando el parte es de alguna extensión.

5.° La rapidez es muy aceptable. Según Carmona, 60 minutos en cifrar mil letras; según Núñez, 73 minutos. En esta clave sucede que por su mucha extensión no pueden aprenderse de memoria los lu-

gares, como pasa en las de letras; por lo tanto con la práctica poco se reduce el tiempo empleado.

6.° No son admisibles los procedimientos de suma, resta o cambio de cifras de que hablan algunos para el caso de haber sido copiada la clave, porque son casi inútiles.

7.° En la práctica resulta muy aceptable su indescifrabilidad. Sin embargo, contadas 10.000 sílabas, he aquí el resultado obtenido en las sílabas dominantes. (Núñez)

A	468	da	99
de	355	los	99
y	278	pa	97
en	260	co	94
que	236	lo	91
E	203	su	90
la	189	mo	86
do	187	ti	85
ci	181	re	84
se	171	ro	84
es	163	ri	83
O	145	sa	83
el	142	na	81
to	138	cu	77
ra	137	so	77
ta	135	an	75
te	135	ha	73
di	134	ma	72
no	122		
ca	109		
con	105		
si	105	40	5.628

En 40 sílabas intervienen 5.628 letras.

Donde vemos que sólo con 40 sílabas tenemos más de la mitad de las 10.000 y que la proporcionalidad está más determinada que en los bigramas.

En evitación de esto, Carmona da tres números a las sílabas

A, de, E, I

y dos números a las

Y, en, que, la, ci, se, es, O, el, ra, U.

Naturalmente esto dificulta mucho el desciframiento furtivo.

La Convención telegráfica internacional acepta como palabra todo grupo de 10 letras que sea pronunciable; y a los

organismos como Embajadas, Consulados, etc., grupos de 10 signos. De modo que si con 5 cifras nosotros expresamos (con el Código que manejamos) una frase, podemos con los 10 guarismos que nos da derecho la palabra telegráfica decir dos frases en que indudablemente con un buen Código, caben muchas cosas.

En los Códigos modernos se usan grupos de 5 letras, que se llaman "grupos códigos".

Los Códigos cifrados tienen las siguientes ventajas sobre los criptogramas:

a) Más seguros que cualquier cifrado, es decir, máximun de seguridad.
b) Economía en la transmisión telegráfica.
c) Rapidez y facilidad de operación para aquellas frases que ya están codificadas.
d) El desciframiento de un grupo código comprometería sólo ese grupo, pero no todo el Código.

Los criptogramas tienen las siguientes ventajas sobre los Códigos:

a) Se puede mantener más secreto que un Código y requiere menos trabajo para su preparación. Por más precauciones que se tengan, un Código puede caer en manos extrañas.
b) La clave y sistema de cifrar pueden cambiarse fácilmente, no así un Código, que exigiría una nueva edición.
c) Se puede cifrar en el mensaje lo que exactamente quiere decirse, lo que no siempre puede hacerse con el Código, donde habrá que recurrir a la tabla de deletreo.
d) Puede ser usado por espías o personal militar que cayese prisionero, puesto que la palabra clave puede retenerse en la memoria.

Una vez elegido el sistema a emplearse, habrá que observar las siguientes reglas si se utiliza el de sustitución:

a) Sustituir la letra E y aquellas de mayor frecuencia en el texto a cifrar, por muchas letras o grupos de letras a fin de escapar al criptoanálisis por frecuencia.

b) Evitar la repetición de sílabas y palabras iguales en el texto a cifrar, para evitar el factoreo.

c) Suprimir las letras dobles "rr", "ll", etc., que caracterizan ciertas palabras del idioma.

d) Utilizar en la sustitución alfabetos incoherentes.

Si el sistema es de transposición hay que observar:

a) Conocer suficientemente las particularidades del idioma, para evitar el empleo de palabras formadas por grupos de letras susceptibles de permitir el análisis de bigramas y trigramas corrientes. Tratar de suprimir la "Q" que siempre va seguida de "U" (una "Q" y una "U" separadas por cuatro letras en el criptograma nos dice que la clave tiene cinco letras), suprimir las terminaciones "on", "cion", etc.

b) Formar cuadros incompletos.

Normas a tenerse en cuenta para cualquier cifrado:

1.ª No hacer nunca cifrados parciales, es decir, no cifrar sólo una parte del texto ordinario.

2.ª Evitar que varios despachos a cifrarse comiencen o terminen con la misma palabra.

3.ª No repetir bajo un mismo sistema o enviar cifrado un despacho que haya sido transmitido en otra forma.

4.ª No transmitir nunca en forma cifrada una clave o una explicación relativa al modo de cifrar.

5.ª Cambiar frecuentemente la clave.

6.ª Utilizar claves variables o interrumpidas.

7.ª No cifrar la firma.

8.ª Escribir el texto a cifrar con faltas de ortografía.

Diccionarios.—Condiciones esenciales de todo buen descifrador y de todo sistema criptográfico.

Diccionarios

Hay varios en español, son muy ingeniosos y allí están por orden más o menos natural y de repetición las 30.000 palabras usuales de nuestro idioma.

Para buscar las palabras fácilmente, lleva cada grupo de hojas un registro con el canto cortado y la muestra de lo que contiene.

Los grupos de letras están colocados de tal forma que no sería difícil combinarlos de otra manera para hacer cambiar incluso la forma de uso del Diccionario.

Hay tablas de "mil radicales" de verbos regulares, con 6 letras como máximum, y tablas de "100 terminaciones" que tengan a lo más 4 letras para hacer combinaciones.

Como la ley de telégrafos admite sólo 10 signos por palabra, todos los Diccionarios y Códigos se hacen a esa base. Los dos grupos de cinco cifras por palabras se consideran, a su vez, descompuestos en dos partes; la primera, formada por las tres primeras cifras, y la segunda, por las dos últimas.

Pero el uso de los Diccionarios está desechado, pues la principal ventaja obtenida con ellos es la economía en las transmisiones telegráficas, y como ésta se obtiene aun mayor con los Códigos modernos para cifrar y aumentan la rapidez del cifrado y descifrado, se han suprimido aquéllos para darles paso franco y casi único en la Criptografía moderna militar. Así es que se usan los Diccionarios para partes

pequeños y algunos métodos de los explicados de sustitución a doble clave, con clave indefinida y alfabetos incoherentes.

Condiciones de un buen descifrador

Penetración.
Conocimiento de la lengua.
Intuición.
Paciencia y constancia sin límites.
Estudio detenido de los métodos criptográficos.
Conocimientos generales de combinaciones.
Cuantos datos pueda adquirir de las circunstancias y datos o asuntos de los corresponsales o espías.

Son condiciones que facilitarán mucho el desciframiento furtivo.

Los Códigos modernos, análogamente a las claves silábicas, tienen dos partes; una, para "cifrar", y otra, para "sacar del código". La primera, para transmitir frases, siguiendo un orden alfabético, para facilitar el que encontremos lo que deseamos cifrar. Los "grupos códigos" que representan esas frases quedarán, como es lógico, en un orden cualquiera. En la 2.ª parte del Código sucede lo contrario; los números van por orden de menor a mayor, y lo que queda desordenado son las frases que ellos cifran.

Los Códigos militares contienen, además, silabarios, tablas de números, tablas de letras, palabras, frases usuales, listas geográficas, listas de regimientos y numerales de buques propios y extranjeros, jerarquías militares, etc., etc.

Para confeccionar los grupos códigos se emplea la "tabla Garble", mediante la cual se forman grupos que tienen la característica de poseer por lo menos dos letras de diferencia entre uno y el otro inmediato siguiente. Esta tabla, como está formada con arreglo a una ley conocida, permite al que recibe el mensaje cifrado reconstituir un grupo código por si tuviese error en la transmisión. Esto es importante, por-

que evita el rectificar la equivocación sin pedir "repita", que cuesta tiempo y dinero.

En la Criptografía, al revés de los demás actos de la vida, el criterio que debe regir nuestras acciones es la desconfianza; es el modo de obtener éxito en este arte de los jeroglíficos.

En general diremos que los métodos a emplear dependerán sobre todo de las circunstancias; de que los mensajes sean largos o cortos, de que se trate de tropas europeas o coloniales, de que estemos en paz o en guerra, con comodidades o sin ellas. El diplomático, el banquero, el comerciante, el policía, se mueven en un ambiente muy diferente del militar.

Resumiendo

Las condiciones esenciales de todo sistema criptográfico han de ser cuatro:

Sencillez.

Rapidez.

Economía en las transmisiones telegráficas.

Indescifrabilidad.

Esta última, si la consideramos en absoluto, es la más importante, pues es la razón de ser de la Criptografía. Analicémoslas por su orden.

Sencillez.—La apreciación de esta cualidad depende de las condiciones del que la juzga, pero no hay duda de que un método, en general, es más sencillo que otro cuantas menos reglas haya que tener en cuenta en su aplicación y cuantos menos requisitos requiera su manejo.

Rapidez.—Depende mucho de la práctica de quien hace el criptograma. Es asombroso lo que aumenta la rapidez unos días de práctica. En claves no muy grandes, y que la vista las domine todas, la rapidez depende de la habilidad de quien las maneja; en otros métodos, con claves de mayor tamaño,

la práctica no hará aumentar tanto la rapidez, pues no será posible que la vista domine de una vez toda su superficie.

No hay que olvidar que todo hay que escribirlo *claro* y *sin prisa,* pues lo contrario puede ser origen de error, que es lo peor que nos puede pasar.

Como datos curiosos sacados de un Gabinete Criptográfico entrenado, diremos que para criptografiar un parte de 1.000 letras debe tardarse (término medio):

Para escribir el parte de 1.000 letras.....	13	minutos
" criptografiarlo	72	"
" rectificarlo y copiarlo en limpio	100	"
Total	185	"

Dividiendo el parte en 4 grupos se gana tiempo, pero requiere más personal. Los criptogramas deben hacerse siempre por dos grupos distintos, para comprobar. Deben ponerse en limpio las cartillas según van siendo criptografiadas.

Suponiendo que el "secreto" y el número de personas disponibles lo permiten, porque si no, debe hacerlo todo el jefe a quien corresponda.

Economía.—Está muy ligada a la rapidez, que antes analizamos. En la milicia, se fija principalmente en la de tiempo.

De la bondad del Código depende casi todo.

Y, por último,

Indescifrabilidad.—Es la más importante.

Como en las anteriores, entra por mucho la parte personal. Las "ideas felices", que resuelven casi milagrosamente los más complicados criptogramas, no están sometidas, naturalmente, a reglas fijas.

Los criptogramas, a la larga, todos son descifrables; su dificultad está en razón directa del número de letras que necesitamos para descifrarlos. Esto es, si un método es doble difícil que otro, quiere decir que si el primero logramos des-

cifrarlo haciendo un estudio sobre 100 palabras, para el segundo necesitamos 200.

Para la práctica consideramos indescifrables aquellos que se resisten al más hábil, cuarenta y ocho horas; para los fines militares nos basta, desde luego, pues ya no tendrá eficacia el conocer lo que se dijo.