Sucinta idea de los diferentes sistemas en que se basa la Criptografía

Por ANDRES MARTIN GARCIA

No son muchas las personas que tienen una idea exacta de lo que es en realidad la Criptografía. En general se la considera como un arte complicadísimo y algo misterioso, pero para los que a través de los años hemos llegado a familiarizarnos con ella nos atreveríamos a decir que sólo constituye un pequeño enigma, que casi podríamos comparar con el que se nos presenta cuando tratamos de resolver uno de los múltiples problemas de matemáticas.

Creemos innecesario hacer resaltar la importancia de la Criptografía, ya que son bien conocidos los eficaces resultados obtenidos en nuestra Guerra de Liberación, y más recientes aún los magníficos servicios que viene prestando a las fuerzas beligerantes en el actual conflicto mundial.

Su empleo fué utilizado ya en la antigüedad por griegos y romanos, los cuales se valían de medios muy curiosos, limitándose todos sus métodos al lenguaje convenido. En la Edad Media se introdujeron los alfabetos de perturbación sencilla, resultando más eficaces que el procedimiento anterior, pero sin ofrecer ninguno de ellos la garantía de conservar el secreto. Se puede decir que la era criptográfica empieza verdaderamente en la Epoca del Renacimiento, en que ya empezaron a utilizarse los llamados Diccionarios o Códigos secretos conjuntamente con las tablas cifradoras y descifradoras que han constituído, hasta hace poco tiempo, con diferentes variaciones, las características más salientes de dicha materia.

Cabe la gloria de ser el primer investigador en cuestiones criptográficas al abad de San Jaime en Wurtzburgo, Juan Tritemio, autor de dos notables obras publicadas en Oppenheim en el año 1518, tituladas "Polygraphia" y "Steganographia", y sobre cuyos métodos se ha cimentado y evolucionado la criptografía moderna.

En España su empleo data del reinado de los Reyes Católicos, quienes usaban este procedimiento para comunicarse secretamente con su embajador en Inglaterra, doctor Puebla, llegando a adquirir un gran desarrollo en el reinado de Felipe II. Don Diego Fernández de Palencia versa también sobre esta materia en uno de los capítulos de su libro publicado en Sevilla en el año 1571, titulado "Historia del Perú". Pero se puede decir que el primer estudio completo fué publicado en Madrid en el año 1738 por don Cristóbal Rodríguez, encontrándose también noticias muy eruditas en la obra del P. Andrés Marcos Burriel.

La palabra "Criptografía" se compone de dos palabras griegas: "kryptos" (oculo y "graphein" (escribir), y es el arte que consiste en transformar un texto claro en lenguaje secreto. Dicho arte se basa en tres sistemas fundamentales, de los cuales daremos a continuación una sucinta idea:

1.º **Sistema de transposición.**—Comprende todos aquellos métodos que, como su propio nombre indica, se limitan a variar o invertir la colocación de las letras del texto claro, dándole un orden convenido que resulte más o menos complicado.

El método de inversión es uno de los más sencillos del sistema de transposición, y consiste en empezar escribiendo por el revés, esto es, empezando por la última letra y terminando por la primera. Fácilmente se puede comprender que este método no tiene utilidad ninguna, pues puede darse el caso, en muchas de las ocasiones, que una misma frase tenga la propiedad de decir lo mismo leída de izquierda a derecha que de derecha a izquierda. Ejemplo: "Anita lava la tina", que colocado según este método, sería: "Anitalavalatina".

Otro método es el llamado de naipes, en el cual se conviene de antemano el orden que han de llevar las cartas en la baraja, escribiendo una letra en cada una de ellas, y si el texto tuviese un número de letras mayor al de las cartas, se vuelve a empezar por la primera, o bien se varía el orden de estas últimas. Una vez terminada esta operación, se barajan bien y se envían al destinatario, el cual las coloca en el orden u órdenes convenidos, descifrando así el texto fácilmente. Como comprenderá el lector, este método es antiquísimo y muy poco práctico, pues habría que disponer de baraja nueva cada vez que se quisiese cifrar.

2.º **Sistema de perturbación o sustitución.** — Este método consiste en el empleo de diferentes letras o cifras, bien utilizando las mismas para cada letra igual o variándolas según el convenio establecido.

En la antigüedad fué muy empleado por los romanos el llamado alfabeto Julio César, basado en este sistema, y que consiste en representar cada letra del texto claro por la que se encuentra en el alfabeto colocado en forma circunferencial y en el sitio convenido. Cifremos, por ejemplo, la palabra "Madrid"; habiendo convenido en representar cada una de las letras del texto claro por la que ocupa el tercer lugar a su derecha en el orden alfabético, tendremos el siguiente criptograma: "Odgulg".

Uno de los métodos más empleados para formar alfabetos perturbados es el de las claves numéricas. Para la formación del citado alfabeto hay que elegir primero una frase clave, dándole a las letras de esta frase su valor numérico. Si elegimos como frase clave "Avionetas", su valor numérico será el siguiente:

A V I O N E T A S
1 9 4 6 5 3 8 2 7

Una vez obtenido el valor numérico de la frase clave, se colocan las letras del abecedario por su orden en los lugares que indican los números, volviendo a empezar por el 1 a cada nuevo renglón en la siguiente forma:

1 9 4 6 5 3 8 2 7
a i d f e c h b g
j q m ñ n l p k o
r . u x v t z s y

Y colocándolas ahora por líneas horizontales, obtendremos el siguiente abecedario perturbado:

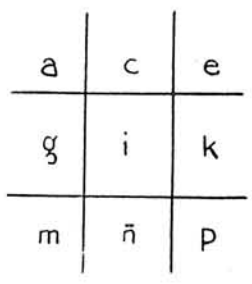
A B C D E F G H I J K L M N Ñ O
a i d f e c h b g j q m ñ n l p
P Q R S T U V X Y Z
k o r u x v t z s y

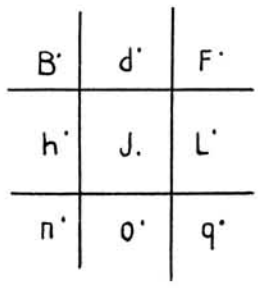
Y si con este alfabeto cifrásemos "EFECTUADO BOMBARDEO, resultaría:

E C E D X V = A F P I P Ñ = I A R F E P.

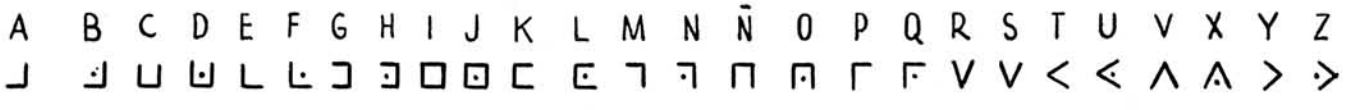
Método de Comercio.—Basado en el método anterior, pero mucho más sencillo, pues nada más hay que designar una palabra de 10 letras que no estén repetidas y darles un valor numérico a cada una, para una vez efectuada esta operación hacer las marcas, siendo las dos últimas los céntimos y las anteriores las pesetas. Este método lo utilizaban mucho los comerciantes para ocultar el precio mínimo a que podían vender sus géneros.

Alfabeto masónico.—Los francmasones para sus comunicaciones secretas tienen formado un alfabeto, consistente en figuras geométricas cuyos signos están basados en lo siguiente:





constituyendo el siguiente alfabeto:



Este método, como puede suponer el lector, sólo puede ser utilizado por carta u otro medio análogo, ya que es imposible transmitir las figuras por radio, telégrafo, etc.

Método de perturbación variable o múltiple.—Son muchos los alfabetos usados mediante este sistema, con objeto de no representar con un mismo signo las mismas letras del texto que se desea cifrar. Entre ellos se encuentra el ideado por el Capitán alemán Hirsch en 1884, que viene a tener las mismas características del llamado método Tritemio. Dicho método consiste en colocar horizontalmente las letras del alfabeto, y con la clave elegida, que puede ser de cuatro, seis o más letras, se forman tantos alfabetos como letras tenga dicha frase clave, empezando cada uno de ellos por las diferentes letras de la frase clave y continuando por orden alfabético hasta concluir.

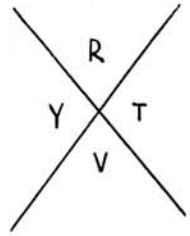
Si elegimos como frase clave la palabra "Rosi", tendremos:

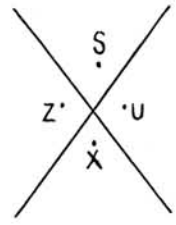
	A B C D E F G H I J K L M N Ñ O P Q R S T U V X Y Z
R	r s t u v x y z a b c d e f g h i j k l m n ñ o p q
O	o p q r s t u v x y z a b c d e f g h i j k l m n ñ
S	s t u v x y z a b c d e f g h i j k l m n ñ o p q r
I	i j k l m n ñ o p q r s t u v x y z a b c d e f g h

El texto claro se divide en grupos de cuatro letras o por tantas como tenga la clave, y se criptografía con el abecedario "R" las primeras de cada grupo, con el "O" las segundas, con el "S" las terceras y con el "I" las cuartas.

3.º **Sistema vario.**—En este sistema se incluyen todos los métodos que no tengan cabida en ninguno de los dos anteriores: diccionarios, lenguaje convenido, libros, etc.

Método silábico.—Usado con menos frecuencia que los demás métodos, es, sin embargo, un procedimiento sencillo y bastante seguro. El Cardenal Torriggiani lo utilizó empleando un número de tres cifras para cada sílaba y sumando o restando, según se conviniese, para no repetir las mismas.





Diccionario de Darhan. — Llamado así por ser el nombre de su autor. Se compone de 30.000 palabras por orden alfabético, numeradas correlativamente desde el 00001 al 30.000. Si dicho Diccionario se limitase únicamente a representar cada palabra por el número de cinco guarismos que se encuentran a su derecha, éste no constituiría ningún secreto; por ello, el autor recomienda para asegurar su eficacia varias combinaciones, de las cuales citamos a continuación las principales:

1.º Alterar el orden de colocación de las tres últimas cifras, convirtiendo, por ejemplo, el número 14.628 en el 14.286.

2.º Sumar un número arbitrario y alterar después la colocación de las tres últimas cifras de la suma (primera y tercera, combinadas).

3.º Añadir a la primera palabra el número de los que componen el texto que se desea cifrar; a la segunda, el duplo; a la tercera, el triple, etc., etc.

Método mixto.—Llamado de esta manera por emplear simultáneamente diferentes signos criptográficos para las letras del alfabeto, para algunas sílabas y para ciertas palabras.

En esta clase de métodos, y por regla general, se suele dar preferencia a las palabras; si éstas no existen, se forman con las sílabas, y por último, se acude al abecedario siempre que no haya otra manera de formar la palabra que necesitamos.

Este método, sin duda alguna, ha sido el más generalizado entre los Gobiernos de Europa durante muchísimo tiempo, ya que su empleo reúne bastante seguridad y es de fácil formación, debiéndose utilizar con preferencia las sílabas y letras de abecedario para hacer más difícil el descifrado.

Lenguaje convenido.—Este no ofrece ninguna particularidad, y solamente se limita a tener un código con las palabras más corrientes que para cada caso se requieran, dándoles otro sentido diferente al de su origen.

Como ejemplo de este método citaremos un hecho curioso del citado sistema: En la correspondencia relativa al complot organizado por el príncipe Luis Napoleón en 1831, se encontró una nota de su puño y letra que contenía una lista de las palabras convencionales adoptadas por los conjurados para designar las personas y cosas que tuvieran que citar con más frecuencia. A la Reina Hortensia se la designaba por M. Antoine; al príncipe Luis Napoleón, por madame Carlos; Inglaterra, por madame Lirson; los bonapartistas, por madame Gock; el Ejército, por mademoiselle Amelia, etc., etc.

Hemos tenido ocasión de exponer en este pequeño resumen una idea de los diferentes sistemas básicos, y quizá muy a la ligera, los cimientos en que se funda la Criptografía.

Actualmente, España, consciente de la gran labor desarrollada por los Gabinetes de Cifra y considerando la enorme importancia que éstos tienen tanto en la guerra como en la paz, cuenta con un buen plantel de criptógrafos distribuídos en los diferentes Gabinetes, preocupándose constantemente de perfeccionar este servicio, de vital importancia para todo país.

La labor del criptógrafo no se limita únicamente a la rutinaria fórmula, que bien pudiéramos llamar mecánica, del cifrado o descifrado. La base principal de todo buen descifrador consiste en el estudio de los múltiples métodos y medios para conseguir el descifrado de un despacho criptográfico cuya clave desconoce. Una de las primeras circunstancias que se deben tener en cuenta para descifrar un escrito es la proporción en que entran las letras del idioma en que esté redactado. Claro es que esta proporción nunca puede ser exacta, sino más o menos aproximada. En español las letras que más se repiten con relación a las demás son: e, a, o, n, s, i: esto hace se pueda operar con mayores probabilidades de éxito.

Todo descifrador hábil acabará siempre por averiguar el método y la clave; pero para esto se necesitan condiciones especiales, y sobre todo mucha costumbre en el manejo de criptógramas de distintos sistemas o claves.

El gran criptógrafo M. H. Josse dice que las cualidades que deben concurrir en todo buen descifrador deben ser "naturales" y "adquiridas".

Entre las "naturales" figura una paciencia a toda prueba y perseverancia para no desalentar en las tentativas que haga, debiendo estar dotado de un gran espíritu de observación para no abandonar los indicios que puedan conducirle a la localización de la clave que busca. La discreción debe ser absoluta, pues de ello depende la seguridad de los métodos empleados.

Entre las "adquiridas" se encuentra una de las más fundamentales, que es la práctica, ya que es indudable que un criptógrafo, con varios años de servicio, domine a la perfección los diferentes métodos empleados, llegando con ella a ser un perfecto técnico en la materia. Cuanto mayor número de conocimientos posea, más fácil le resultará y estará en mejores condiciones para ejercer su cometido, debiendo dominar las siguientes materias: **Literatura, Matemáticas, distintos procedimientos criptográficos y un conocimiento muy vasto del idioma que emplee.**