Criptografía y descriptación

Por el Teniente BUENO TREJO

Criptografía es el arte de escribir enigmáticamente.

Esta forma de escribir también recibe los nombres de criptología, poligrafía, esteganografía, escritura cifrada y algunos más, según sean sustituídos los signos alfabéticos por cifras, signos musicales, algebraicos, o bien por signos arbitrarios, letras de un idioma, por caracteres propios de otro o por otros del propio alfabeto, bien sean letras sencillas o en grupos de dos o más.

La escritura cifrada, diplomática o de clave, es llamada así por su uso corriente en Embajadas, Legaciones y otros servicios dependientes de las mismas. Las fuerzas armadas emplean corrientemente la cifra o criptografía, recibiendo el nombre de "Criptografía militar".

Todos los sistemas, por raros que parezcan, y todas las estratagemas que se utilizan para el curso de mensajes, órdenes, noticias, etc., y que tengan un carácter reservado, entran de lleno dentro de la criptografía.

Tomemos, por ejemplo, la fuga de vocales, la escritura con tintas simpáticas, los signos que algunos vagabundos graban en los árboles y fachadas de las casas, el lenguaje de las flores y otros muchos muy variados. Todos forman parte de esta ciencia, pero solamente nos ocuparemos de su forma en la parte concerniente a los caracteres o signos gráficos. Y haciendo un poco de historia veremos que Julio César fué uno de los que más utilizó este sistema de escritura, ideando una forma de cifrar que consistía, y consiste (pues aún se utiliza), en anticipar el valor o la equivalencia de otras cuatro de la letra que se ha de cifrar; así que al escribir la letra A tendríamos que presentarla con la letra D, y así sucesivamente dentro del orden alfabético.

Condiciones que debe reunir un sistema o método criptográfico.

Debe ser material, si no matemáticamente indescifrable, que no exija el secreto, pudiendo sin inconveniente caer en poder del enemigo, que sea fácil de comunicación y suceptible a la retentiva mental del cifrador para evitar notas escritas y poderlas cambiar o modificar a voluntad de los corresponsales. Asimismo debe poderse emplear utilizando los medios de comunicación modernos, de fácil manejabilidad y que solamente tenga que intervenir una sola persona en su manejo.

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

Las obras de Carmona, Núñez Losada y otras, pueden servir de ejemplo a lo anteriormente citado.

Las características especiales que tiene la criptografía militar requiere que el personal destinado en los Gabinetes de Cifra posea una gran práctica, pues muchas veces se han de transmitir órdenes que han de ser cumplidas inmediatamente. Por tanto, el que cifre o descifre debe efectuarlo con la mayor rapidez y seguridad. Un Jefe de Estado Mayor del Ejército, en un libro recientemente publicado, dice: "En un curso de criptografía al que asistan varios oficiales hay que tener en cuenta que a la terminación del mismo solamente serán utilizables la mitad, y de éstos, seleccionar", circunstancias que no se precisan en otros Gabinetes, aunque también cifren.

El cifrador que tiene que efectuar su trabajo bajo el fuego o la presión enemiga, no cabe duda que no puede efectuarlo con la misma tranquilidad que en un Gabinete; por tanto, no es nada difícil que cometa algún error, dificultando la labor de interpretación del criptograma, y más aún si tiene

necesidad el que lo recibe de pedir rectificación, con lo que sufre gran retraso el cumplimiento de las órdenes mencionadas en el mensaje, con las consiguientes consecuencias.

Las claves y los códigos deben ser reducidos y los menos posibles, pues en caso de fuerza mayor o de abandono de la posición en que se opera, hay que llevarlos consigo o proceder a su destrucción por medio del fuego, ya que podían caer en manos del enemigo. Los Gabinetes permanentes permiten el empleo de claves y códigos de mayor volumen o aparatos mecánicos de tamaños varios y en el número de éstos que se consideren necesarios, ya que en los citados despachos o Gabinetes hay muebles a propósitos para ser guardados. Por otra parte, existe la prohibición absoluta de intromisión de personas ajenas a este servicio en las dependencias donde están instalados.

En la Gran Guerra estos Gabinetes estaban instalados en cámaras acorazadas, y desde allí los Oficiales de Estado Mayor, y por conexiones eléctricas, transmitían sus signos criptográficos fuera de estas cámaras secretas.

La Criptografía consta de dos partes:

La gráfica y la analítica, criptoanálisis o descriptación.

La analítica permite descifrar un mensaje hasta conseguir su traducción completa.

Para la operación de cifrar un despacho no es preciso poseer unos conocimientos especiales, pues cualquiera puede confeccionar un criptograma.

Ahora bien: la operación de cifrar ha de hacerse empleando bien las claves y sacándolas todo su rendimiento, pues del mal uso o empleo de una clave o código depende la mayoría de las veces que un mensaje sea descifrado.

Por tanto, la operación de cifrar se debe hacer con rigurosa atención y meticulosidad, procurando evitar las repeticiones o haciéndolo lo menos posible, sustituir unas palabras por otras de significación igual o parecida, a criterio del cifrador. Esto sólo lo puede hacer un especialista en la materia, y no es fácil que éstos cometan errores.

Para descriptar, no conociendo la clave ni el método empleado, se requiere personal muy especializado, principalmente en el conocimiento de idiomas, sistemas de cifrado y reunir unas condiciones que más adelante veremos con más detenimiento.

Métodos y sistemas criptográficos.

La seguridad de un criptograma depende de la frecuencia del cambio de claves.

Los sistemas fundamentales que se utilizan para cifrar son:

El sistema de sustitución y el de transposición. Más adelante veremos con un ejemplo el funcionamiento de este sistema.

Los alfabetos utilizados en criptografía constan frecuentemente de veinticinco letras; con ello permite confeccionar un cuadro completo, ya que es múltiplo de 5, y estaría compuesto de cinco columnas de cinco letras cada una y por el mismo número de líneas y letras.

En estos alfabetos se suprimen las letras LL, Ñ y W, que se consideran como mudas.

Criptográficamente, los alfabetos están considerados como escritos en círculo cerrado.

Claves y métodos.—Las claves pueden ser limitadas o ilimitadas.

Las claves de letras pueden convertirse en números, o inversamente.

Códigos.—En la actualidad, dados los sistemas tan rápidos de transmisión (radio, teletipo, etc.), para expedir textos largos con el menor número de grupos posible, suelen usarse códigos, diccionarios o libros, utilizándose también palabras aisladas como base de una clave.

El manejo de estos códigos es sumamente sencillo y rápido, y tienen la particularidad de ser poco susceptibles a equivocaciones, como asimismo pueden conceptuarse como indescifrables.

Para el descifrado de estos códigos suelen usarse tablas de sistemas varios.

Sistema de sustitución y sistema de transposición.

En el primero se sustituyen las letras del texto en claro por otras o por cifras, y en el segundo se emplean las mismas del texto en claro, pero trastornadas. Estos sistemas son vulnerables a la descriptación, y por tanto, poco seguros.

Mensaje cifrado con el sistema de sustitución.

Primera operación.—Cifrado:

YHJDXDDQJVWWHXFJHSOYHGSGJGOT
QVERPLB

Segunda operación.—Formarlo en grupos para facilitar su transmisión:

BLPRE-UQTOG-LGSGH-YOSHJ-FXHWW-
VJQDD-XDJHY-XVSGC

Para el cifrado de este despacho se han utilizado cinco alfabetos, y se ha transmitido inversamente, como puede apreciarse.

Con el fin de dar mayores probabilidades de seguridad a los criptogramas, debe procurarse eliminar en lo posible la frecuencia del idioma, dando a las letras de más repetición tantas representaciones como se pueda.

Sistema Porta.

Este sistema consiste en una tabla compuesta de once alfabetos recíprocos de veintidós letras:

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

Como puede verse en esta tabla, de las veinticinco letras normales del alfabeto han sido suprimidas la j, k y l.

En este sistema la frecuencia o repetición desaparece, ya que es a doble clave.

Al aparecer este sistema de cifrado (siglo XIV), dicen los historiadores que causó una revolución en el arte de cifrar, por lo que se le llamó el padre de la criptografía moderna.

Tabla de Vigenere.

Esta tabla, ideada por Blaisse Vigenere, es bastante más perfecta que la de Porta, pues con ella desaparecen las imperfecciones de ésta.

Consta de veintiséis alfabetos normales ordenados, y lo mismo puede usarse verticalmente que horizontalmente (en la actualidad sigue empleándose).

Método de transposición o perturbación.

En este método, como ya sabemos, no se emplea letra alguna nueva; tan sólo nos servimos de las del mensaje que se ha de cifrar, mezclándolas entre sí, como puede apreciarse en el siguiente ejemplo:

Texto a cifrar: AVIONES CAZA SALEN PARA ESE FRENTE.

Se busca una palabra clave. En este caso	A M A P O L A
Y se le da a cada letra un valor.	1 5 3 7 6 4 2
Debajo, y horizontalmente, se escribe el texto	A V I O N E S C A Z A S S A L E N E S E F R E N T E - -

Una vez confeccionado el criptograma, expediríamos el mensaje por columnas dentro del orden de los números y en sentido horizontal:

1-5-3-7-6-4-2

1 2 3 4 5 6 7
ACLR-SAFI-ZNNE-SEVA-EENS SEOA-ETE

Este método de cifrar es muy vulnerable a la descriptación, ya que buscando el divisor del número total de letras del criptograma, nos dará el número de las que se compone la clave. Escribiendo el cifrado en tiras de papel y haciéndolas coincidir unas con otras, se llega a sacar el claro del mismo.

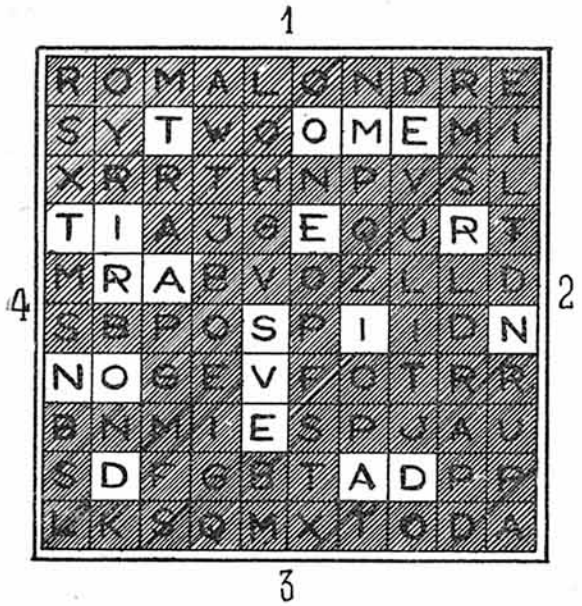
También puede ocurrir que el mensaje esté escrito unas columnas de arriba abajo y otras en sentido inverso; pero de todas formas, puede llegarse a su descifrado.

En la criptografía militar se debe procurar por todos los medios posibles que no sean fácilmente descriptables los textos expedidos, o por lo menos, complicarlos de tal forma que su descriptación obligue al empleo de varias horas de trabajo, a fin de que la eficacia de su contenido pierda todo su valor.

Sistema de rejillas.

Este sistema, bien empleado y construída la rejilla con ingenio, es dificilísimo de descriptar.

Consiste en abrir unas ventanas en un papel o cartulina, corrientemente de forma cuadrada, en cuyas ventanas, y sobre otro papel de forma similar, se escribe el texto



en sus cuatro posiciones, rellenando los espacios libres con letras o palabras puestas a capricho. Este sistema es aplicado en páginas de libros señaladas de antemano, en revistas, periódicos, etc., etc. Si los que utilizan la clave son solamente dos personas, expedidor y consignatario, o viceversa, es casi de todo punto imposible su captación, a no ser por alguna confidencia.

Máquinas de cifrar.

Aparatos automáticos.—El sistema mecánico de cifra en la actualidad, en que existen aparatos automáticos de una perfección tan grande y de unas probabilidades de seguridad tan ilimitadas que materialmente es imposible descifrar ningún mensaje llevado a cabo con este sistema, ya que efectúan las sustituciones por miles y millones de veces. Suponiendo que varias máquinas buscaran la descriptación de un mensaje, haciendo combinación tras combinación, tardarían años, y caso de poder, al fin, poner el mensaje en clave, éste habría perdido, por tanto, todo el valor que tenía cuando se transmitió.

Muchos y muy variados son los sistemas de cifrado que existen, y para poder dar una ligera explicación de su funcionamiento, haría falta un voluminoso texto; por tanto, nos limitaremos a esta pequeña referencia dada sobre los mismos, y pasaremos a la criptoanálisis o descriptación.

Criptoanálisis o descriptación.

Una de las bases más fundamentales para la descriptación furtiva de un criptograma, consiste en efectuar un profundo y detenido estudio sobre la proporcionalidad de las letras que con más frecuencia se repiten en los distintos idiomas, como asimismo de los bigramas, trigramas, etc. "Ley de Frecuencia".

En español, por ejemplo, las frecuencias han sido registradas en la siguiente proporción: Por mil,

E	A	O	S	M	R	I	L
132,99	126,41	93,50	78,20	68,14	63,42	55,31	49,72

Las terminaciones más frecuentes en español corresponden a las terminaciones masculinas, femeninas y a los plurales O, A y S. Asimismo, las terminaciones mente, sísimo, ción y fico.

Dado lo rico en palabras del idioma español, se hace verdaderamente complicada la descriptación de un cifrado no poseyendo dato alguno sobre la clave o método empleado.

Todas las reglas y métodos que existen para descriptar tienen como base la Ley de Frecuencia.

Los criptogramas, cuanto más extensos son, más factibles de descifrar, e inversamente, cuanto más cortos, más difíciles, ya que la frecuencia de letras, bigramas o trigramas es muy limitada.

Dentro de estos criptogramas, los menos costosos de descriptar son los comerciales o aquellos en que las repeticiones de cifras es casi constante; en los comerciales no es solamente la repetición de números, sino de mercancías, taras y puntos de destino, etc.

A pesar de los métodos existentes para el descifrado de mensajes, los cuales pueden servir indudablemente de base, la práctica ha enseñado que los propios y exclusivamente personales, la constancia y la paciencia sin límites, no son la mayoría de las veces las que dan la solución del enigma.

Las sustituciones a doble clave, con alfabetos perturbados, son prácticamente indescifrables. Asimismo los códigos sin ordenar y algún que otro sistema llenan las necesidades militares más corrientes.