**Reproducción de un capítulo dedicado a la Criptografía en un libro de Táctica de la Academia de Ingenieros del Ejército de 1957.**

---

# PRIMER GRUPO T Á C T I C A

## CUARTA PARTE

## ORGANIZACIÓN Y EMPLEO DE LOS INGENIEROS

## T E M A 88
## CRIPTOGRAFIA

**Programa:-Definición. - Terminología. - Sistemas criptográficos. - Ejemplos. Protección de las transmisiones**

### -1.-Definición

La palabra Criptografía, se deriva de las voces griegas "Kriptos", escondido y "Graphein", escribir, y sirve para, designar el arte de escribir enigmáticamente, con objeto de impedir que quien no posea la clave penetre en su significado. Hoy el concepto de Criptografía, es mucho más amplio y puede definirse corno, el arte de cifrar y descifrar, o sea, escribir enigmáticamente o convencionalmente por medio de clave y leer o interpretar dichas escritos.

La Criptografía se fundamenta en el principio general y evidente de que es mucho más fácil inventar una escritura secreta que interpretarla.

La Criptografía recibe también los nombres de poligrafía, esteganografía, escritura cifrada, diplomática, de clave, etc.

### -2.-Terminología

En Criptografía se utilizan diversas palabras, cuyo significado interesa precisar y conocer. Entre los más usuales tenemos las siguientes:

- **Clave o cifra** se llama a la variante del método, es decir, al acuerdo convencional y transitorio las más veces, con arreglo al cual se cifra o se descifra por un método cualquiera. La clave puede ser numérica o alfabética, sencilla o, doble.

- **Cifrado**r es el que cifra.

- **Cifrar, cifrado, o ciframiento** es una operación que consiste en transformar en texto claro en enigmático o secreto.

- **Corresponsales** se denominan las personas que utilizan en sus comunicaciones la criptografía.

- **Criptografiar** equivale a cifrar, es decir, consiste en aquella operación que permite transformar un texto o mensaje claro en otro cifrado o enigmático.

- **Criptografista** es la persona versada en criptografía y especialmente en el cifrado y descifrado de criptogramas conociendo la clave.

- **Criptógrafo** se denomina al aparato empleado para, cifrar o descifrar en los métodos que así lo requieren.

- **Criptograma** se denomina al texto o escrito secreto.

- **Criptología** es la parte de la criptografía que tiene por objeto el descifrado de criptogramas ignorando la clave.

- **Criptólogo** se llama a la persona versada en criptología, es decir, en el descriptado de criptogramas, o sea el descifrado desconociendo la clave y el método por que fueron cifrados.

- **Descifrar, descifrado o contra-cifra**, es la operación inversa a la de cifrar o cifrado, es decir, la que consiste en transformar el texto enigmático en comprensible por medio de la clave.

- **Descriptar, descriptado o descriptamiento** es la operación que consiste en averiguar el contenido de un escrito secreto ignorando la clave. También se denomina perlustración.

- **Lenguaje cifrado** se llama al enigmático o secreto.

- **Lenguaje claro** se denomina al normal o al que se obtiene una vez descifrado o descriptado un criptograma,

- **Lenguaje convenido** es aquél cuyas palabras poseen un sentido convencional distinto del gramatical.

- **Lenguaje mixto** es el que resulta de combinar el normal o claro con el convenido o con el cifrado.

- **Lenguaje secreto** se denomina al lenguaje cifrado o convenido.

- **Letra obligada** con respecto a otra es aquella que inevitablemente la sigue en los escritos, como, por ejemplo, la U es obligada con respecto a la Q, en castellano.

- **Letra repetida** se dice de aquella, que en el lenguaje original puede ir duplicada, como por ejemplo, la LL y la RR, etc.

- **Letra o signo anulante**, se dice del que tiene la propiedad de dejar sin valor a los elementos que le proceden o le siguen,

- **Letra o signo inerte** es el que, careciendo de todo valor o representación, se interpola en los criptogramas con objeto de dificultar su descriptado.

- **Letra o signo nulo** es aquel que, careciendo de todo valor o representación, se interpola en los criptogramas con objeto de dificultar su descriptado.

- **Letra o signo nulo** es aquel que, careciendo de todo valor, se agrega al texto enigmático en ciertos métodos que requieren un determinado número de signos o representaciones para completarlos.

- **Método** es la designación que recibe cada uno de los procedimientos especiales de cifrado.

- **Monograma** se llama a cada letra o signo aisladamente.

- **Perlustración** es la parte especial de la criptografía que enseña a descifrar ignorando la clave. Este término es sinónimo de criptología y se deriva de su significación mitológica.

- **Perlustrar o perlustrado** equivale a descriptar o descriptado.

- **Poligrama** se denomina al conjunto de letras, cifras o signos que representan una palabra, y también al agrupamiento circunstancial de dos o más de estos elementos. Los poligramas reciben los nombres particulares de **bigramas**, **trigramas**, **tetragramas**, **pentágramas**, **hexagramas**, **heptagramas**, etc., según que consista en la agrupación de dos, tres, cuatro, cinco, seis, siete, etc. letras o signos.

- **Representación enigmática** es la conseguida al sustituir las letras correspondientes al texto claro por las otras letras, cifras o signos que las representan en el criptograma.

- **Representación normal** es la que tiene cada una de las letras de un mensaje antes de ser cifrado después de ser descifrado o descriptado.

- **Sistema** se llama, al conjunto de métodos criptográficos, que, basándose en el mismo fundamento o principio, representan muchos puntos comunes o semejantes.

- **Texto enigmático** es el cifrado secreto.

- **Texto normal** o claro es el comprensible y gramatical.

**-3.- Sistemas criptográficos**

En criptografía las letras o palabras pueden seguir con su valor y representación normales, alterándose solamente su orden, o por el contrario, ser sustituidas por otras letras, cifras o signos, aunque cabe también que ambos medios de cifrado se combinen.

De acuerdo con lo expuesto, en síntesis, todos los métodos criptográficos utilizados y conocidos hasta la fecha pueden considerarse agrupados en tres sistemas perfectamente diferenciables: **Sistema de transposición, sistema de sustitución y sistema mixto**.

**El sistema de trasposición** comprende, como su nombre indica, aquellos métodos que consisten en alterar el orden natural de las letras, sílabas o palabras de un escrito, trastocándolas; es decir, que aun conservando los elementos del texto claro, su representación normal, su orden es modificado.

**El sistema de sustitución**, en un sentido amplio, abarca aquellos métodos basados en reemplazar las letras, sílabas, palabras o frases de un escrito por otras letras o palabras distintas, por guarismos o signos, o por grupos de guarismos o signos; es decir que los elementos del texto claro son sustituidos por una representación distinta a la original. Se ha convenido en llamar sustituciones esteganográficas las que tienen lugar mediante otros caracteres o dibujos que no sean letras ni cifras.

**El sistema mixto**, por último, comprende los métodos que participan de las características de los dos sistemas anteriores; es decir, aquellos en los que el texto claro es primeramente sustituido y luego traspuesto, o viceversa.

**Trasposición sencilla y doble**. - Sus denominaciones indican claramente en qué consisten. La primera es la que tienen lugar cuando el orden de lastras que componen el texto, no experimenta más que una sola alteración; la segunda, o doble, supone una segunda alteración del texto, ya alterado por la primera trasposición.

La trasposición comprende varios sistemas complementarios, entre los que merecen citarse la trasposición por dibujo y por rejilla

**Sustitución simple y múltiple**. También sus nombres expresan su significado. En la primera cada letra del texto es sustituida por otra letra, por una cifra o por un signo; en la segunda, cada letra del texto claro puede ser sustituida por varias letras, cifras o signos.

En la sustitución sencilla o simple quedan comprendidos aquellos métodos limitados a sustituir los caracteres del texto claro por otros caracteres o signos diferentes, que, sin embargo, siguen guardando el mismo orden, o sea, que cada signo será siempre reemplazado por otro específico que lo representará y que ocupará su mismo lugar, como sucede, por ejemplo, en el alfabeto Morse, la escritura, Baille de los ciegos, la masónica, etc.

Si la sustitución tiene lugar por medio de, letras se denominará literal; si por números, numérica, y esteganográfica, si por signos.

Finalmente, los **métodos llamados de libro, los códigos y tablas cifradoras**, etcétera, si bien realmente encajan perfectamente dentro del sistema de sustitución, por no quedar subordinada ésta a un orden riguroso, pueden considerarse agrupados independientemente.

**-4.-Ejemplos.**

**ESCITALO (figura 1)**

Plutarco lo describe así: "Cuando un General parte para una expedición de Tierra o Mar los, éfores (Ministros) toman dos bastones redondos, perfectamente iguales en longitud y grosor, de manera que se corresponda exactamente uno con otro en todas sus dimensiones. Ellos guardan uno de esos bastones, dando el otro al General; y llaman a

estos bastones Escítalos. Cuando quieren evitar al General un secreto de importancia, portan una tira del pergamino larga y estrecha como una correa, arrollándola alrededor del escítalo que guardaron, sin dejar el menor, intercalo entre los bordes de la banda, de tal suerte que el pergamino cubra enteramente la superficie del bastón. Sobre este pergamino así arrollado del escítalo, escriben lo que desean y después quitan la cinta y la envían al General sin el bastón. El General que la recibe no sabría leerla porque las letras, perdida la alineación y dispersas, no tendrían continuidad; pero el tomo del escítalo que llevó consigo y arrollando alrededor la banda del pergamino, se reunirán las vueltas volviendo las letras a tomar el primitivo orden en que fueron escritas. Esta misiva se llama escítalo, del nombre mismo del bastón, como aquéllo que se mide toma el nombre de aquéllo que le sirve de medida.

**Método de Julio César**

Este antiguo método está comprendido entre los de sustitución o desplazamiento, llamándose de Julio César, en atención a quien lo inventó y lo usó. Consiste en dos alfabetos normales, uno de, ellos doble, que se acopla convenientemente a otro sencillo.

Para cifrar, basta resbalar el segundo por el primero, uno o más lugares, tantos corno indique la clave, e ir sucesivamente sustituyendo cada una de las letras del texto a cifrar, que las buscaremos en el alfabeto sencillo por sus correspondientes del alfabeto doble.

Sea por ejemplo que deseamos cifrar con clave tres. En este caso cada letra del escrito a cifrar irá representada por aquélla que le siga tres lugares; es decir, que el alfabeto cifrador quedará desplazado tres lugares con la relación al correspondiente del texto claro, así, la A irá representada por la D, la M por la O, etc.

```
Alfabeto Normal  : A B C D E F G H I J K L M N Ñ 0 P Q R S T U V X Y Z.

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

Luego la frase ESPERAME MAÑANA quedaría representada por el siguiente Criptograma:

3-HVSHUDOH ODQDPD.

Para descifrar bastará operar en forma inversa, sustituyendo sucesivamente cada una de las letras del texto enigmático por aquéllas que les precedan tres lugares.

Algunos autores afirman que Julio César utilizaba los discos concéntricos, girando uno de ellos, uno, dos o más lugares, tantos colmo indique la clave, basta luego ir sustituyendo las letras. En realidad, el procedimiento es idéntico en ambos casos.

**METODO VIMBOIS**

Consiste en convenir:
-un alfabeto
-un número clave.

Hecho ésto, se escribe el texto original y, debajo de cada línea, el número clave repetido tantas veces sea necesario.

Para cifrar se corren tantos lugares en el alfabeto como indica en la cifra que cae debajo de la letra considerada.

Para descifrar se hace la operación contraria.

Por ejemplo, empleando:
- el alfabeto normal del ejemplo anterior
-el número 1635 como clave,

si queremos cifrar: ATAQUEN PRIMER OBJETIVO tendríamos
A T A Q U E N P R I M E R O B J E T I V O
1 6 3 5 1 6 3 5 1 6 3 5 1 6 3 5 1 6 3 5 1

que daría, el texto cifrado
B A D V V K P U S Ñ O J S U E Ñ F A L B P
que se transmitiría en grupos de cuatro letras, para aumentar la confusión
B A D V - V K P U - S Ñ O J - S U E Ñ - F A L B - P

Para descifrar los grupos
E E V V - M Ñ N S con la clave 243
tendríamos
2 4 3 2  4 3 2 4
E E V V  M Ñ N S
C A S T  I L L O

## ANEXO AL TEMA 88
## Protección de las Transmisiones

El empleo imprudente de las Transmisiones permite al enemigo informarse sobre nuestras operaciones actuales y futuras, anulando todo efecto de sorpresa.

Se impone, por consiguiente, la adopción de medidas que aseguren la protección de las Transmisiones contra la exploración enemiga por el adversario.

### MEDIDAS GENERALES

**Mantener el secreto de las comunicaciones, a toda costa, constituye una cuestión de honor para el personal de Transmisiones.**

**Todo individuo perteneciente al servicio de Transmisiones**, cualquiera que sea su categoría, está obligado a:

- guardar una absoluta reserva sobre todo lo que haya llegado a su conocimiento a consecuencia de su peculiar misión; no debe hacer, ni ante los propios compañeros del Servicio, comentario o alusión al contenido de los telegramas, conversaciones telefónicas y sobre la personalidad de los corresponsales.

- evitar por todos los medios que la correspondencia telegráfica y de documentación de las estaciones pueda caer en manos del enemigo o quedar al alcance de persona, militar o no, que no esté autorizada a inspeccionarla por razón de su cargo.

- persistir en la conducta indicada aún en el caso de caer prisioneros.

- queda terminantemente prohibido el acceso a las estaciones y Centros de Transmisiones, a toda persona, ajena al servicio excepto la autoridad militar de quien dependan y personas debidamente autorizadas.

La permanencia en su proximidad inmediata no se permite ni aún a los ordenanzas afectos a ella.

**Al Mando**, y en general a todos los usuarios del Servicio de Transmisiones corresponde:

- Mantener la debida discreción sobre las operaciones en estudio o en período de desarrollo.

- Custodiar celosamente la correspondencia, especialmente durante su transporte entre los Puestos de Mando y los Centros de Transmisiones.

- Emplear preferentemente el lenguaje cifrado, ajustándose siempre a las normas dictadas para su uso; principalmente en las comunicaciones radioeléctricas.

**En todas circunstancias**, dentro de la zona de los Ejércitos:

-Se prohíbe a la población civil la comunicación por telégrafo, teléfono, o radio, palomas mensajeras y medios ópticos. Únicamente en casos excepcionales podrá el Mando autorizar ciertas comunicaciones telefónicas o telegráficas en determinadas condiciones.

-La correspondencia Postal se autorizará en las condiciones que fije el Mando, el cual suspenderá, secuestrará u ordenará su censura si lo cree conveniente.

- Se explotará la existencia de todos los medios susceptibles de facilitar el espionaje: instalaciones de escucha telefónica, aparatos de radio, teléfonos clandestinos, palomas mensajeras, etc.; todo militar que sospeche su existencia, está obligado a denunciarla, sin demora.

La escucha, de las Transmisiones propias permite al Mando comprobar si se observa una estricta disciplina en el servicio de Transmisiones.

## MEDIDAS PARTICULARES

En todos los escalones, el Mando debe ordenar medidas adaptadas a la situación, para la protección de las, Transmisiones.

Estas medidas tienden a conseguir la invisibilidad de las instalaciones, su protección contra el fuego y la defensa técnica contra la escucha enemiga.

## INVISIBILIDAD,

Para, que las instalaciones sean menos perceptibles a la observación enemiga terrestre y aérea, se precisa:

- disimular los trabajos relativos al establecimiento de las Transmisiones, evitando modificar el aspecto del terreno;

- evitar en lo posible que se perciba la convergencia de muchas líneas en los Centros de Transmisiones, enterrando, si es preciso, algunos circuitos para no denunciar la importancia de la estación y del Puesto de Mando a éste aneja;

- reglamentar los movimientos de ida y vuelta de los agentes de enlace y ordenanzas en las proximidades de los Centros de Transmisiones y Puestos de Mando.

**Protección, contra el fuego**

Siempre que sea factible, especialmente en períodos de estabilidad, las estaciones y Centros de Transmisiones deben instalarse en abrigos a prueba de proyectiles de artillería y aviación.

Para disimular la vulnerabilidad de los Centros de Transmisiones conviene diseminar todo lo posible sus elementos, siempre que con ellos no se perjudique la rapidez y la coordinación de empleo de dichos elementos.

En las zonas expuestas a una acción intensa de las armas indicadas las líneas telegráficas y telefónicas deberán enterrarse a profundidad suficiente para protegerlas, de la onda explosiva. Con el mismo fin las comunicaciones alámbricas esenciales debe mantenerse por varias líneas trazadas por distintos itinerarios.

**Defensiva técnica**

Para proteger las, transmisiones propias contra los efectos de la escucha enemiga se precisa.

- Mantener una rígida disciplina en la ejecución de los servicios, haciendo cumplir estrictamente las disposiciones del “Reglamento para la Explotación de las Transmisiones”.

- Un inteligente empleo de códigos y claves cifrado, cuidando especialmente de no transmitir nunca en lenguaje claro números y nombres de Unidades o de Mandos, ni indicaciones sobre los efectos y distribución de fuerzas.

- Limitar el uso de los medios de Transmisión a lo estrictamente indispensable.

**TRANSMISIONES ALAMBRICAS**

Para dificultar la escucha por inducción deben evitarse los circuitos unifilares con vuelta por tierra en la zona de vanguardia, prohibiéndolos en absoluto en períodos de detención y defensiva, aunque sea momentáneamente. Estas líneas son admisibles solamente durante rápidos avances que no permitan al enemigo organizar con regularidad sus servicios de escucha.

Con los mismos fines, los dos conductores de cada línea deben estar muy próximos entre sí, recomendando para las líneas más próximas al enemigo el trazado de cable.

Las líneas aéreas se construirán, en todos les casos, con sistemas anti-inductivos, sistemas que se ejecutarán también en toda la línea que se habilitó eventualmente para comunicaciones telefónicas. (Líneas de alumbrado, transporte enrgía, telegráficas, etc ... ).

Deben ser localizadas y reparadas las averías que, aunque no impiden la comunicación (aislamientos defectuosos, derivaciones a tierra, etc.), facilitan notablemente la escucha.

Toda instalación que haya cesado de ser necesaria o útil será desmontada. Se revisarán con frecuencia y minuciosidad todas las líneas en servicio y sus proximidades, para explotar si existen derivaciones o ramales de escucha por inducción destinados a sorprender nuestras comunicaciones.

Las centrales y los Mandos deben ser designados por contraseñas que se cambien con frecuencia.

En país enemigo, las Centrales y las líneas deben separarse de las localidades habitadas por la población civil.

Las conversaciones particulares entre telefonistas y personas no autorizadas para ello deben ser prohibidas en absoluto.

Aunque en la construcción y entretenimiento de las líneas se observen escrupulosamente las precauciones indicadas, es poco discreto el uso del teléfono en vanguardia, por lo cual no se prodigará en ella este medio, llegando, cuando se suponga que el enemigo dispone de un buen servicio de escucha, al aislamiento de los circuitos avanzados, y hasta la prohibición del empleo del teléfono en ciertas zonas precintando los aparatos para restringir su uso a los casos de reconocida urgencia. Los observatorios instalados en estas zonas peligrosas, deberán utilizar el teléfono con las máximas precauciones, telefoneando sus indicaciones, en forma que el enemigo no pueda sacar partido de ellas.

En cada caso, se fijarán las zonas en que es obligatorio el cifrado de telegramas y telefonemas o el uso de aparatos de transmisión secreta, así como las medidas relativas a la variación de contraseñas.

No se utilizará ninguna instalación existente sobre el campo de batalla sin un examen previo destinado a comprobar que no puede ser interceptada por el enemigo o sus agentes que hayan podido quedar a retaguardia de nuestras propias fuerzas.

Para evitar su utilización en instalaciones de escucha las Tropas de Transmisiones tienen obligación de cortar todas las líneas, (telefónicas, telegráficas, de transporte de energía, etc.) que se dirijan hacia el enemigo; pero los cortes deberán efectuarse en forma que no impidan una rápida reparación en caso de avance.

Ante una posible retirada se tendrán previstos los repliegues de líneas que se estimen factibles y la destrucción de los restantes del material telefónico y telegráfico que no pueda ser transportado asignando a cada individuo con claridad su misión en estos casos.

## TRANSMISIONES RADIOELECTRICAS

En la utilización de estos medios de transmisión se precisa mantener, hasta la exageración, una disciplina extremada en el cumplimiento de las reglas de explotación, prohibiendo toda relación no oficial entre los operadores, así como toda fantasía o particularidad en la manipulación, por constituir todo ello un precioso material de informes para la localización de las Unidades por el enemigo.

Por la misma causa deben, en principio, prohibirse los telegramas, circulares y el sistema de trabajo en correspondencia dirigida.

Por la extrema facilidad de su captación por el adversario, debe limitarse el uso de la radio, en todos los casos a lo estrictamente indispensable llegando a prohibir su empleo en la concentración, aproximación y demás circunstancias en que sea de máximo interés la conservación del secreto.

Toda Red Radio deberá mantener la consigna de: Hablar poco, escuchar mucho.

Sin orden expresa, firmada por la Autoridad a que afecta la situación, no se transmitirá ningún radiotelegrama cuyo texto no esté completamente cifrado.

Las Estaciones transmisoras, especialmente las que por sus características denuncian claramente la Autoridad a que está afecta, se alejarán convenientemente de los Puestos de Mando, ligándolas telefónicamente a ellas.

Las longitudes de onda y los indicativos deberán cambiarse con mayor frecuencia posible y con arreglo a un plan de conjunto empleando los indicativos de enlace, con, referencia a los de estación.

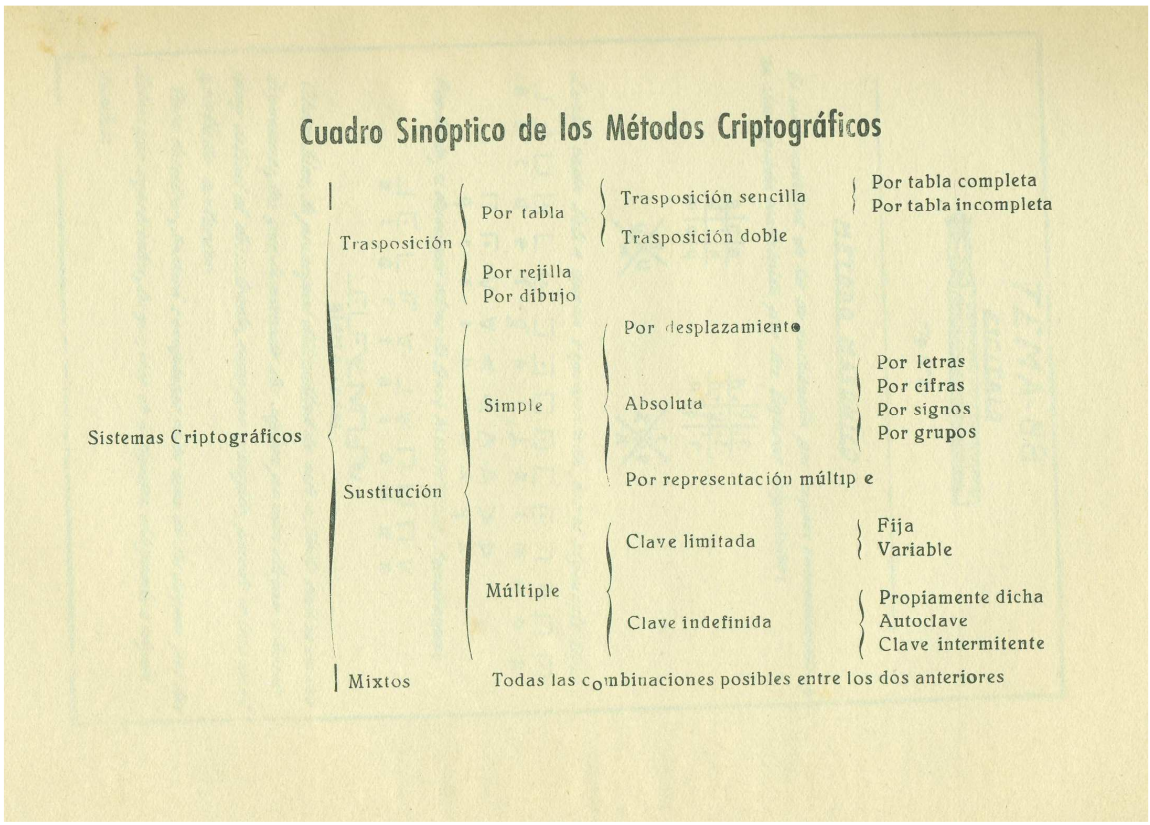
Los Jefes de Transmisiones en los diversos escalones del Servicio, vigilarán con sus Estaciones de escucha el exacto cumplimiento de las anteriores normas del trabajo.

## TRANSMISIONES OPTICAS

Hay que procurar evitar el empleo de los medios ópticos en los enlaces normales al frente reservándolos para las comunicaciones transversales. Cuando se precise comunicar en dirección al enemigo, se observarán las precauciones indicadas para la transmisión de radiotelegramas.

No debe emitirse más intensidad de luz que la necesaria para que las señales sean percibidas por la estación receptora para lo cual se emplearan en los aparatos de luces, sistemáticamente las pantallas de diafragma y vidrios colorados

Cuando se empleen, artificios de luces deben variarse con frecuencia los códigos y los lugares de lanzamientos de cohetes y cartuchos de señales, pero procurando evitar estos cambios en períodos de actividad del frente, en los que pueden dar lugar a confusiones.



# TEMA-88

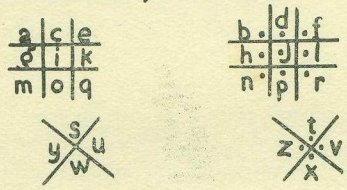
## ESCITALO

Fig. Nº 1

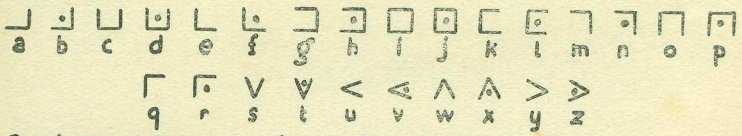
---

## METODO MASONICO

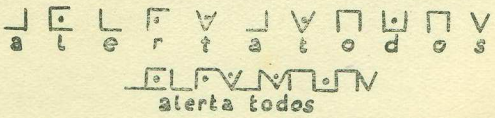
Es una variedad de los de sustitución por signos convencionales, y su clave queda constituida por las figuras siguientes:




Luego cada letra queda representada por el siguiente signo:




Por tanto, si deseamos cifrar la frase ALERTA TODOS, tendremos:




Ahora bien, la principal dificultad de este método radica en sus ligaciones, las que sucediendo los signos pueden llegar a hacer muy difícil el descifrado, como por ejemplo, puede verse en el grabado anterior.

Para descifrar, bastará reemplazar cada uno de los signos por las letras que representen, las que, caso de las ligadas, obligarán a algún tanteo.