BREVE BOSQUEJO HISTORICO DE LA CRIPTOGRAFIA

La CRIPTOGRAFIA, que según el Diccionario de la Real Academia, consiste en el "arte de escribir con clave secreta o de un modo enigmático", es tan antigua como la Humanidad misma. Su etimología proviene del griego (kriptos, oculto y graphein, escribir) y nada tiene que ver con la HERMENEUTICA ó arte de interpretar, por lo que no debe confundirse.

El proceso historico de la Criptografía seria objeto de un estudio muy amplio y que no viene al caso, por lo que es suficiente con un bosquejo de las etapas mas características, que podemos dejar reducidas a siete:

1.- La escritura en la antigüedad.-

- Inscripciones (hititas, etruscos,....), verdadero enigma criptográfico que sigue sin resolverse, puesto que aún no han sido descifradas.
- Jeroglíficos (persas, egipcios, babilónicos, mayas,.....), que han podido ser ya todos descifrados.
- Escrituras , correspondientes a distintos pueblos o razas y que abarcan toda la complejidad de lenguas y civilizaciones que se asentaron entre el Eufrates y el Tigris muchos años a. de J.C.: asiria, caldea, meda, persa,.....

Hay que hacer constar el trascendente paso que se dió para llegar a descubrir gran parte de las inscripciones jeroglíficas y escrituras egipcias, gracias a la lammada "Piedra de Roseta", encontrada en Egipto durante las campañas de Napoleon. La escritura jeroglífica egipcia, no se empleaba mas que en los monumentos públicos o privados; en la vida ordinaria, los egipcios se servian de otra mas cirsiva, derivada de la anterior, y que hoy recibe el nombre de "hierática"; mas tarde, se simplificó mas aún y surgió una nueva escritura, de utilidad tambien comercial, llamada hoy "demótica" ó "popular". Pues bien, allá por el año 1.798 un Oficial francés, llamado Boussard, encontró en el fuerte de San Julian de Roseta, un trozo de piedra en el que estaban grabadas, una debajo de otra, tres inscripciones: la superior en caracteres jeroglíficos;la del centro, en demóticos, y la inferior, en griego. La famosa piedra fué a parar a Londres y figura en el Museo Británico. Sobre ella comenzaron a trabajar los mejores descriptadores del mundo, pero fué el orientalista francés Juan Francisco Champollion quien llegó a la conclusión, mediante un detallado estudio de las tres inscripciones, de que cada uno de los caracteres hieratico y demótico (se auxiliaba con otras inscripciones traidas de Egipto) no eran sino estilizaciones del jeroglifico; por fin en 1821 logró descriptar la palabra jeroglífica correspondiente a la griega "Ptolomis"(Ptolomeo) y, tras ellas, los nombres de Berenice y Alejandro. De esta forma llegó a conocerse la, hasta ahora, enogmatica historia egipcia.

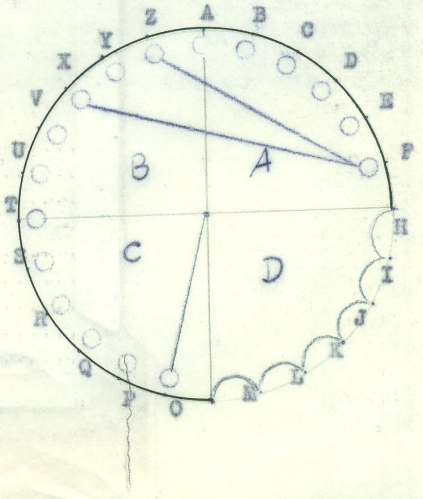
2.- Epocas históricas antiguas.-(alrededor de J.C.)

-Cifra bíblica.- Empleada para designar nombres de personajes o lugares geográficos.

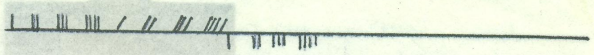
-Estratagemas de Grecia.- A Herodoto se deben las reseñas que nos han llegado para conocer algunas "estratagemas"que usaron en su época. Una de ellas consistia en introducir la misiva en el vientre de una liebre,método este empleado por Ciro con ocasión de destronar a Astiages, rey de los medos; Ciro necesitaba de algunos informes y su cómplice Harpago se los envió en el vientre de una liebre y que un cazador llevaba con otros en su morral.
Otra estratagema consistia en rapar a un esclavo, y sobre su afeitada cabeza escribirle - con tinta indeleble - el mensaje; esperar a que creciera el pelo y mandar al esclavo. Esto parece que se puso de moda, pero con una variante; tatuar el mensaje y despues de cumplida su misión cortar la cabeza del esclavo (?)

-Tabletas enceradas.- Empleadas en Roma y que consistian en grabar el texto en ellas y despues recubrirlas de una fina capa de cera para ocultarlo.

-Plancheta de Eneas.- Consistente en un disco dentado - cuadrante D de la figura - o con orificios; cada diente u orificio representaba una letra. Un hilo salia del centro e iba pasandose por los orificios según la letra que se quisiera representar; el destinatario deshacia el ovillo e iba obteniendo las letras del texto en sentido inverso



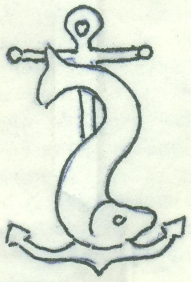
-Ogams celtas.- Cuyos vestigios son muy abundantes en los paises nórdicos.



A B C D E F G H I J K L .....

-Scytalo lacedemonio.- Inventado y utilizado por los griegos de Esparta y que podemos considerar como el mas antiguo método de transposición, y aún como primera maquina cifradora que en el mundo ha sido. Cuando un general espartano partia para una expedición de tierra o mar, los "eforos" tomaban dos bastones cilindricos, perfectamente iguales en longitud y grueso, de manera que se correspondiera el uno con el otro en todas las dimensiones. Guardan ellos uno y entregan el otro al general.
Cuando quieren enviar algún secreto de importancia cortaban una banda de pergamino y la enrollaban alrededor del "Scytalo" de forma tal que lo recubriese totalmente. Sobre el pergaminto así arrollado escribian lo que deseaban y lo enviaban al general sin bastón. El general que lo recibia, enrollaba el pergamino y podia leer con claridad.
Así nació el actual bastón de mando militar, convirtiendo en un simple símbolo jerárquico lo que en su origen fué una útil maquina cifradora.

-Anagramas.- Pertenecen a la Criptografia apostolica. En la primera figura aparece un pez - simbolo de "Jesús, Cristo, Hijo de Dios, Salvador - ensartado con un ancla - recuerdo de la Cruz - y por un tridente -Santisima Trinidad- respectivamente. En la segunda figura vemos un báculo o bastón pastoral y la cruz episcopal, simbolo con el que los apóstoles representaban el poder espiritual transmitido por Jesucristo.



f

-Julio César.- Consistente en un alfabeto desplazado conrespecto a otro un número determinado de lugares y que se utilizaba para sustituir al alfabeto normal.

De todos ellos, puede decirse que el "scytalo" lacedemonio constituye el precursor de los métodos de transposición, y el "Julio César" del de los de sustitución.

3.- Edad Media.-

-Fuga de vocales.-Solo se cifran las vocales y estas son reemplazadas por uno, dos, tres, cutaro o cinco puntos ó cruces. Ejemplo: DOMINUS.....

-Alfabetos cifrantes.- Sustitución de letra por signo o número , lo que no le resta semejanza con el Julio César.

4.- Siglos XV y XVI.-

-Repertorios cifrantes.- Tablas de correspondencia donde las palabras eran sustituidas por signos. No se cifraban todas las palabras, y en un principio no eran mas allá de 120. Conforme fué aumentando el número de palabras que era preciso cifrar, los signos se reemplazaron por números (generalmente de 3 cifras).

-Tratados de Criptografía.- Bellaso y Porta en Italia, Tritemio en Alemania y Vigenere en Francia, comienzan a utilizar varios alfabetos cifrantes y crece el interés por esta materia.

Por esta época aparecieron los primeros "gabinetes de cifra" y se iniciaron los trabajos de descriptación.

5.- Siglo XVII.- Podemos considerarlo como el Siglo de Oro de la Criptografía y en el que ésta adquirió su mayor apogeo. Aparecen los Códigos, y dos figuran ejercen un preminente papel: Lord Bacon y Rossignol. Francis Bacon, en Inglaterra, es el inventor de la cifra biliteral. Hay quien asegura de que Lord Bacon no es otro que el propio Shakespeare. Antoine Rossignol, en Francia, trabajó para Richelieu, Luis XIII, Ana de Austria, Luis XIV y Mazarino (naturalmente antes que con el Rey Sol). Rossignol es el "as" de la cifra y de la descripación y prestó grandes servicios a Francia, llegando a descriptar, sobre el terreno, mensajes que permitieron a los franceses éxitos militares. Su facilitad y aptitudes para romper claves fué tal, que los descuideros siguen llamando "rossignol" o "ruiseñor" a las ganzuas para abrir lo cerrado u oculto.

En este siglo hicieron su aparición los Códigos.

6.- Siglos XVIII y XIX.- Periodo de decadencia para la Criptografía que perdió parte del gran impulso recibido en el siglo anterior.
Se pierde la cifra a nivel de gobierno y se utiliza para comunicaciones entre personajes políticos o entre empresas comerciales.
La Criptografía pasa a ser el lenguaje de las flores, de los abanicos, etc. y a formar parte de la literatura (Balzac, Poe,....)

7.- Finales del siglo XIX y siglo XX.- Vuelve la Criptografía a adquirir importancia. Casi todos, o todos, los Estados crean sus escuelas criptográficas. Aparece otro importante personaje inglés creador del llamado método Playfair, método que aún está en uso.
El desarrollo de los medios de comunicación y transmisión dan fuerte impulso a la cifra.
Aparecen los Diccionarios y se pone en práctica el recifrado.
Por último, otro impulso se debe a las máquinas criptográficas y a la aplicación de los ordenadores.

S E G U R I D A D C R I P T O G R A F I C A

DEFINICION : La Seguridad Criptográfica se puede definir como el conjunto de medidas tendentes a garantizar el secreto de las comunicaciones cifradas.

CÓMO SE LOGRA? La Seguridad Criptográfica se logra mediante una adecuada elección de los sistemas de cifra más idóneos en cada caso, su utilización de la forma más conveniente y su protección en todo momento. Todo éllo, - con objeto de impedir o dificultar en el grado mayor posible la inteligencia de las comunicaciones cifradas propias a quien no corresponde.

Vamos a analizar un poco cada uno de estos conceptos :

ELECCION DEL SISTEMA CRIPTOGRAFICO.-

Los requisitos que debe reunir un Sistema Criptográfico no son fijos. Dependen del fin a que se destine, de los diferentes factores que intervienen en cada situación o planteamiento y de los que puedan preverse.

Las cuestiones que ineludiblemente deben realizarse en los distintos planteamientos que se presenten, son las siguientes:

- El grado de seguridad que debe alcanzarse.
- Los medios criptográficos con que se cuenta para establecer el sistema.
- El medio o medios de transmisión a utilizar para enviar los mensajes.
- La urgencia media que se requerirá a la comunicación. Máximo tiempo - exigido para el cifrado, la transmisión y el descifrado de un mensaje.
- Las condiciones físicas de seguridad de los Gabinetes de Cifra.
- El grado de Especialización del personal.

Hay que formularse siempre las siguientes preguntas:

QUIEN ? Va a utilizar el Sistema.
CÓMO ? Se va a emplear el Sistema.
DÓNDE ? Se va a utilizar.
CUANDO ? Durante cúánto tiempo estará en vigor.
CON QUÉ MEDIOS ? Contamos para implantar el Sistema.

GRADO DE SEGURIDAD QUE DEBE ALCANZARSE.-

Se refiere a la seguridad intrínseca del Sistema Criptográfico que se adopte. Dado el avance de la técnica criptográfica y considerando un empleo perfecto de todos y cada uno de los Sistemas, se pueden considerar como indescriptables, con las reservas que una afirmación de esta índole entraña, los mensajes cifrados por "cinta aleatoria" y los producidos por criptógrafos electrónicos que autogeneran series "pseudo aleatorias".

..././/...

En principio, el grado de Seguridad de un Sistema Criptográfico depende:

- Del número de textos cifrados.
- Del tiempo que se mantiene en vigor.
- Del tiempo mínimo que se calcula ha de necesitarse para su descriptación.

Pero lo más importante a considerar es el CÓMO se va a emplear el Sistema elegido, QUIENES lo van a utilizar y QUÉ protección se le da.
Tán importantes son estas cuestiones que pueden hacer falsa la afirmación hecha anteriormente de ser indescriptables textos cifrados por "serie aleatoria" o "pseudoaleatoria".
Visto lo anterior, se llega a la conclusión de cómo están de íntimamente relacionadas la Seguridad Criptográfica , con la utilización de los Sistemas y con la debida protección de los mismos.
En general se puede afirmar que TODA CLAVE ES BUENA, SI SE HACE UN USO - ADECUADO DE ELLA. Y que la Clave considerada como más segura, deja de ser lo en el momento que se hace un mal uso de élla.

QUE SE ENTIENDE POR HACER UN BUEN O MAL USO DE UNA CLAVE ?

Se hace un mal uso de una Clave si se comete alguno de lo que en los Cursos de Criptografía llamamos "PECADOS CAPITALES CRIPTOGRAFICOS" que son los que aparecen en pantalla. (Descripción de cada uno de éllos).

MEDIOS CRIPTOGRAFICOS CON QUE SE CUENTA PARA ESTABLECER UN SISTEMA.-
Estos medios son muy variables, van desde el equipo electrónico para la comunicación cifrada automática por "serie aleatoria", que utiliza teletipo o radioteletipo para la transmisión, hasta la simple "Clave Manual" que puede utilizar un simple agente y que se sirve para transmitir sus mensajes de técnicas como la del "micropunto".
Podemos establecer una división importante, a saber:

- Sistemas Criptográficos que permiten establecer comunicaciones cifradas entre varios corresponsales, con una misma Clave.
- Sistemas Criptográficos que sólo permiten establecer comunicación cifrada entre dos corresponsales o "punto a punto".

Un estudio constante de los avances de las técnicas modernas aplicadas a la Criptografía, y una sabia y constante política de adquisiciones, harán posible tener en nuestras manos los medios necesarios para ser utilizados de la forma más adecuada a cada planteamiento.

..././/...

MEDIOS PARA LA TRANSMISION DE MENSAJES.-

La cuestión a tener en cuenta en relación con la Seguridad Criptográfica, será la mayor o menor facilidad que tendrá un hipotético "contrario" para captar los mensajes que se transmitan cifrados.

Para establecer una escala de valoración, podemos ordenar los medios de transmisión más usuales de la forma siguiente, en órden de menor a mayor seguridad: Como más indiscretos, la radio y el teléfono. Mayor seguridad, el teletipo, valija transportada y valija conducida.
Como es natural existen subdivisiones en cada uno de estos grupos de medios de transmisión.
Siempre será más segura una transmisión por radio con indicativos en clave variable y variación de frecuencias en cortos períodos de tiempo, que la hecha con indicativos en claro y frecuencias fijas.
De igual forma dá menos garantía una valija transportada cuya custodia se encarga al piloto de un avión de línea regular, que la conducida por una persona entrenada, armada y que lleva la valija esposada, no pudiendo ser abierta mas que por la persona remitente y destinataria.
Se debe recalcar que lo verdaderamente importante es conocer de antemano el grado de facilidad que tendrá el "contrario" para captar nuestros mensajes.

URGENCIA MEDIA QUE SE REQUERIRA A LA COMUNICACION.-

Es muy importante tener en cuenta la urgencia que normalmente tendrán los mensajes cifrados a transmitir, antes de adoptar uno u otro Sistema Criptográfico.
La mayor o menor rapidez en la transmisión y recepción de un mensaje cifrado depende de la suma de dos tiempos: Tiempo de cifrado y descifrado, más tiempo de transmisión. En el caso más favorable se puede considerar como nulo el primer sumando, es decir, el tiempo empleado en cifrar y descifrar; contando naturalmente con los medios necesarios.
Hay que recalcar la importancia de tener en cuenta esta urgencia que va a precisar la transmisión, pues el no hacerlo, lleva, por ejemplo, a que una determinada Autoridad comunique en un momento determinado, por teléfono y en claro, el contenido de un mensaje que ya se ha ordenado transmitir cifrado.
Un hecho de esta naturaleza, obliga a la anulación inmediata de la Clave utilizada y a su sustitución, cuando se tenga conocimiento por el Servicio Criptográfico, porque se ha puesto en peligro la Seguridad del Sistema.

...//...

CONDICIONES FISICAS DE SEGURIDAD DE LOS GABINETES DE CIFRA.-

En síntesis, hay que considerar tres apartados diferentes, para conocer el grado de seguridad que tiene la custodia de los Sistemas Criptográficos:

- El edificio.- Varía si se trata de una edificación permanente, aislada, con guardia militar, etec. o si se trata de una casa situada en el extranjero, por ejemplo.
- La habitación.- Puede ser desde una cámara blindada, con aislamientos anti radiación, situada en edificio oficial, a una simple habitación en un domicilio particular.
- El mueble.- Puede variar desde la caja fuerte con combinación y una sóla llave, hasta el simple cajón de una mesa de despacho.

Independientemente del grado de seguridad que se obtenga para un puesto, es importante tener en cuenta que, cuando se trata de una Red de Cifra - compuesta por varios corresponsales, el grado de seguridad física que tendrá el Sistema de Cifra utilizado, será el mismo del Puesto de Cifra que tenga el menor grado de seguridad. Esto obliga a dotar de los medios necesarios a todos y cada uno de los Corresponsales de la Red.

Como resumen de todo lo expuesto, hay que señalar que siempre que se vaya a adoptar un Sistema Criptográfico, hay que obtener una información lo más completa posible, para contestarnos estas preguntas:

- Qué grado de Seguridad se ha de alcanzar.
- De qué medios de transmisión se dispone.
- Quiénes van a utilizar el Sistema.
- Y dónde van a estar custodiados los Sistemas Criptográficos.

Dejamos para una intervención posterior lo referente al grado de especialización del personal que ha de emplear la Cifra.

- - - - - - - - - - - - - - -

S E G U R I D A D C R I P T O G R A F I C A

"P E C A D O S C A P I T A L E S" C R I P T O G R A F I C O S :

1º.- CIFRAR UN MENSAJE PARCIALMENTE (parte de él va cifrado y parte en claro).

2º.- HACER REFERENCIA EN CLARO, DE FORMA VERBAL O ESCRITA, AL TEXTO DE UN MENSAJE QUE HA SIDO O VA A SER CIFRADO.

3º.- CIFRAR UN TELEGRAMA CUYO TEXTO HA SIDO ENVIADO ANTES EN CLARO, O VICEVERSA.

4º.- CIFRAR DOS O MAS TELEGRAMAS DISTINTOS CON COMBINACIONES DE CLAVE IDENTICAS.

5º.- CIFRAR TELEGRAMAS CON IDENTICOS TEXTOS CLAROS, CON DOS O MAS CLAVES DISTINTAS.

6º.- DAR DIFUSION AL CONTENIDO DE UN TELEGRAMA CIFRADO O DESCIFRADO, SIN HABER ALTERADO PREVIAMENTE SU FRASEOLOGIA (PARAFRASIS) Alterar la redacción sin que varíe el contenido del texto.

7º.- NO DESTRUIR CUANTAS COPIAS, PAPELES, BORRADORES, ETC. HAYAN SERVIDO PARA LAS OPERACIONES DE CIFRAR O DESCIFRAR UN MENSAJE.

- - - - - - - - -

SISTEMAS, METODOS Y PROCEDIMIENTOS CRIPTOGRAFICOS

- SUSTITUCIONES
  - Simples
    - Representación única
      - Letra por letra
      - " " binúmero
      - " " signo
      - Bigrama por bigrama
    - " múltiple
      - Letra por bigrama
      - " " binúmero
    - Códigos
      - Trigrama
      - Cuatrigrama
      - Pentagrama
      - por: letra, número, bigrama, binúmero, palabra, expresión
  - Dobles o Polialfabéticas
    - Clave limitada
    - Clave ilimitada
      - Criptógrafos
      - Cintas serie aleatorias
      - Autoclaves
      - Libro
  - Fraccionamiento
- TRANSPOSICIONES
  - Simples
    - Inversión
    - Cuadro
      - Completo
      - Incompleto
  - Rejillas
    - Fijas
      - Celosía
      - Cuadro casillas numeradas
    - Giratorias
      - Cuadradas
      - Circulares

CONFIDENCIAL