# INTRODUCCION A LA CRIPTOLOGÍA.

## Introducción.

La criptología es el estudio de los métodos y formas de diseñar y romper códigos y cifras utilizados para ocultar el contenido de un mensaje, o el mensaje en si mismo, a personas que no deben tener acceso a él. La criptología se ha dividido clásicamente en tres ramas:

- *Criptografía*. Encargada de diseñar métodos para ocultar el contenido de un mensaje, no el mensaje en sí mismo. Para ello realiza toda una serie de transformaciones en el mismo de forma que sin conocer el origen y desarrollo de éstas, así como una serie de informaciones complementarias, en general la clave, sea imposible conocer el contenido del mensaje original.
- *Criptoanálisis*. Son todos aquellos métodos dedicados a obtener el contenido del mensaje original sin conocimiento de parte de la información requerida para ello, principalmente la clave.
- *Esteganografía*. Son todos aquellos métodos tendentes a la ocultación del mensaje en sí mismo. Forman parte de este grupo las tintas simpáticas, la ocultación de bits de información en imágenes y la técnica de los micropuntos. Sobre este tema existe una amplia bibliografía que va aumentando cada día a medida que se descubren nuevas utilidades a este conjunto de técnicas, marcas de agua, marcas digitales, etc. [WAY93][WAY96b][AND98][AND99].

En una sociedad como la nuestra, basada en la información, la criptografía ha ido tomando una importancia cada vez mayor. La información como recurso, es un bien precioso y como tal debe protegerse adecuadamente, solo debe ser revelada a las personas adecuadas, en el momento adecuado y con el formato adecuado. Pero no solo es en este apartado en el que la criptografía tiene un papel fundamental, sino también en aspectos tan importantes como la autentificación, la integridad y la no repudiación, conceptos estos imprescindibles en aplicaciones tales como el comercio electrónico, la certificación de documentos electrónicos y la transferencia electrónica de fondos.
La criptografía ha pasado por la historia por varias etapas, en cada una de ellas se han realizado avances y se han descubierto debilidades en los métodos utilizados. Podemos dividir estas etapas en:

- *Criptografía clásica*. Antes de la aparición de los trabajos de Shannon. Se utiliza un enfoque más lingüista, recordemos que en la famosa *room 40* la mayoría de los criptoanalistas eran lingüistas expertos y especialistas en crucigramas.
- *Maquinas de cifrado*. Durante la primera mitad del siglo XX. Se utilizan las máquinas de cifrado para eliminar los errores derivados de la complejidad de los nuevos algoritmos de cifrado y aumentar la seguridad de los mismos.
- *Criptografía moderna*. Los trabajos de Shannon se consideran el inicio de la criptografía moderna con un enfoque claramente más matemático. No es que hasta este momento no se hubieran utilizado las matemáticas en criptografía, recordemos los trabajos de Friedman, Turing, Rejewski, Kullback y Sinkov entre otros. Todos ellos eran matemáticos y aplicaron sus conocimientos a la criptografía y al criptoanálisis, siendo algunos de los trabajos de Friedman y de Kullback aplicaciones de la estadística al criptoanálisis. El mérito de Shannon fue el de desarrollar una teoría general de los

sistemas criptográficos basándose en modelos matemáticos, y sobre todo, el ser el primero en poder presentar estos trabajos a la luz pública, ya que los citados anteriormente no pudieron hacerlo al trabajar para el ejército. Sus trabajos solo se conocieron años después, una vez desclasificados.

Si bien los trabajos de Shannon marcan el inicio de la criptografía moderna, el trabajo de Merkle y Hellman es el punto de referencia para la criptografía tal como la conocemos ahora. Si bien en círculos militares [ELL70] ya se conocía el concepto de criptografía de clave pública, es indudable que la aparición de este trabajo, junto con un desarrollo extraordinario de las comunicaciones, han hecho crecer de una manera enorme la popularidad y el interés de la comunidad, tanto científica, como comercial, por el tema.

## Definiciones.

Definimos un alfabeto *A* como el conjunto de símbolos que se utilizan para representar un mensaje, $A = \{a_1,...,a_m\}$. En una operación de cifrado de la información pueden existir uno o varios alfabetos, aunque generalmente se utilizará uno, o dos, uno para el mensaje en claro y otro para el mensaje cifrado, pueden llegar a utilizarse varios.

Definimos un *n-grama* como el nuevo alfabeto generado por la utilización de combinaciones de *n* elementos de un alfabeto de *m* símbolos, siempre con $m \geq n$. En los casos $n = 2$ y $n = 3$ hablaremos respectivamente de *digramas* y *trigramas*.

Definimos una función, o método de cifrado *E* como un conjunto de transformaciones no triviales sobre elementos del conjunto de mensajes *M* dando como resultado un elemento del conjunto de posibles mensajes cifrados *C*. La transformación *E* debe ser invertible y llamamos a este proceso *D*. Ambos procesos *E* y *D* utilizan unas informaciones complementarias $k_e, k_d \in K$, denominadas claves, y no necesariamente distintas.

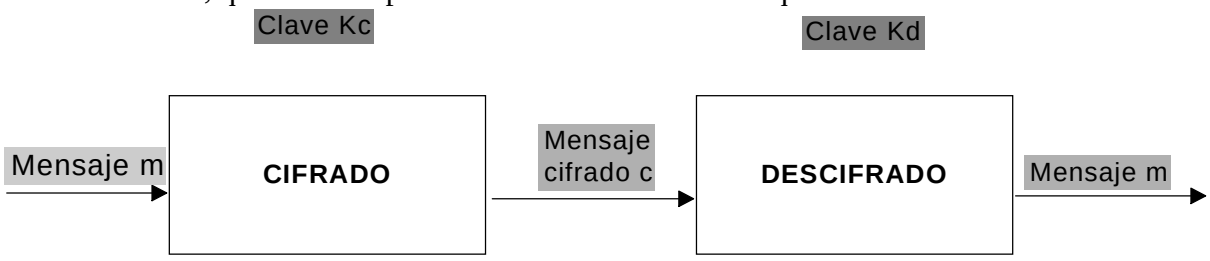
A la aplicación de las operaciones *E* y *D* la denominamos *cifrado* y *descifrado* de la información respectivamente y suponemos que son realizadas por el personal autorizado a ello y por lo tanto con el conocimiento de las respectivas claves $k_e, k_d \in K$. Es posible la obtención del mensaje en claro sin el conocimiento inicial de la clave de descifrado. A la obtención de esa información por otros medios, así como la obtención de la clave de descifrado se denomina criptoanálisis* para diferenciarla del descifrado con conocimiento legal de la clave. Si el criptoanálisis de los mensajes puede realizarse de una forma sistemática o con una probabilidad muy alta, se dice que se ha *roto* el código.

En algunos textos se suele utilizar la palabra codificar para el proceso de cifrado. La utilización de la palabra código y de la codificación de un mensaje en claro solo puede ser aceptada en el caso de la utilización de un libro de códigos, ya que un código, es en general la representación de un determinado ítem (palabra, carácter, etc..) mediante un neumónico y su función principal, si exceptuamos el caso de los libros de códigos, es la representación de la información de una forma más adecuada para su procesamiento. En la criptografía actual se utilizan los códigos como un paso intermedio en el cifrado para permitir el tratamiento de los datos en sistemas de computo o comunicaciones.

* En la criptología clásica se denomina descriptación al criptoanálisis.

# Sistema criptográfico.

Dado un mensaje *m* (utilizamos la notación criptográfica, en realidad un mensaje puede ser un fichero, un campo, un registro o una Base de Datos entera), unas claves de cifrado $k_c$ y de descifrado $k_d$, que pueden ser la misma, y unos métodos de cifrado *E* y de descifrado *D*, que también pueden ser el mismo tenemos que:




De una manera más formal definimos un criptosistema como una tupla de cinco elementos (*M*, *C*, *K*, *E*, *D*) tales que se cumplan las siguientes condiciones:

1. *M* es un conjunto finito de posibles mensajes.
2. *C* es un conjunto finito de posibles mensajes cifrados.
3. *K* es el conjunto de todas las posibles claves.
4. Para todo $k_1$ perteneciente a *K*, hay una regla de cifrado $E_{k_1}$ perteneciente a *E* y una correspondiente clave $k_2$, no necesariamente distinta de $k_1$, y regla de descifrado $D_{k_1}$ perteneciente a *D*, tales que $E_{K_1} : M \to C$ y $D_{k_2} : C \to M$ son funciones que cumplen $D_{k_2}(E_{k_1}(x)) = x$ para todo mensaje *x* perteneciente a *M*.

Las funciones *E* y *D* pueden implementarse mediante sistemas de cifrado o bien mediante libros de códigos.

Una definición más intuitiva obtenida de [CAR94] es la siguiente:

> Llamaremos *sistema* al conjunto de métodos que, por tener un mismo origen ó fundamento, están basados en un mismo género de combinaciones y tienen una cierta semejanza entre sí; *método*, á la serie convenida de operaciones para transformar un texto claro en lenguaje secreto, de una manera más o menos complicada, y *clave*, á las variantes que pueden introducirse dentro de cada método, sin modificar su fundamento esencial.

Se dice que un criptosistema moderno es seguro si cumple las siguientes condiciones [DEM81], siendo la última no estrictamente necesaria pero muy útil en ciertos protocolos:

1) Para cada mensaje *M*, tenemos que $D_{k'}(E_k(M))=M$.
2) $E_k$ es computacionalmente tratable.
3) $D_{k'}$ es computacionalmente tratable.
4) *D* está protegido de un enemigo que conoce *E*, es decir *K*, pero no *K'*, por un problema computacionalmente intratable.
5) Para cada mensaje *M*, tenemos que $E_k(D_{k'}(M))=M$.

## Elección de un sistema criptográfico.

Existen una gran variedad de sistemas de cifrado, desde algunos sumamente sencillos, como el de Julio Cesar, a otros muy sofisticados y potentes como AES, IDEA o RSA. La elección de un método u otro depende de varios factores principalmente de:

1) *Vida útil de la información*. Si la información solo es útil durante minutos e incluso segundos, es posible que se sacrifique seguridad por rapidez en el cifrado. En este caso el ataque al sistema solo debe realizarse en el caso de disponer de información privilegiada que nos permita suponer un cierto éxito, en caso contrario, el ataque solo puede ser útil para obtención de información sobre los métodos utilizados y frecuencias de cambio de claves y controles administrativos que se realizan sobre los datos en aras a intentar un ataque posteriormente. Por el contrario si los datos mantienen su validez durante mucho tiempo, es prácticamente seguro que se emplearan métodos muy potentes y complejos de cifrado de forma que el ataque sea muy costoso. En este caso se dispone de tiempo, si bien no ilimitado, si mucho mayor que en el caso anterior, por el contrario el mero intento de criptoanalizar estos datos obligará a una inversión en tiempo y material mucho mayor.
2) *Entorno de trabajo*. Es inútil aplicar métodos complejos de cifrado si todos los usuarios que deben recibir la información no disponen de material para procesarlo. Es muy útil comprobar el estado de los sistemas en todos los puntos a los que se envía el mensaje cifrado, es posible que en alguno de ellos se disponga de material criptográfico de menor fortaleza y permita el criptoanálisis de una forma más sencilla.
3) *Tipo de aplicación*. Uno de los mayores condicionantes en la elección del sistema criptográfico es el tipo de aplicación que va a utilizar la criptografía. En algunos casos, cifrado y descifrado de información en tiempo real, consultas a bases de datos en línea, la velocidad de operación es determinante, sin embargo, en este último caso, es tan importante el hecho de que los datos cifrados no aumenten el tamaño del original, ya que esto obligaría a continuas reorganizaciones de la base de datos.

## Objetivos de la criptografía.

Si bien el objetivo inicial de la criptografía ha sido históricamente la obtención del secreto en las comunicaciones, paulatinamente se han añadido una serie de objetivos a medida que crecían las necesidades de comunicación y aparecían nuevas posibilidades. Podemos citar entre otras los siguientes propiedades deseables en un sistema criptográfico [RIV**].

1) *Confidencialidad.* Nadie excepto los comunicantes deben poder conocer el texto del mensaje.
2) *Autentificación*. El receptor quiere estar seguro de la identidad del emisor del mensaje.
3) *Firma digital*. Uno de los comunicantes quiere convencer a una tercera persona de que el mensaje fue enviado por el otro.
4) *Minimalidad.* La comunicación, fuera del ámbito de los comunicantes, es nula.

5) *Intercambio simultaneo* de información entre comunicantes, por ejemplo en la firma de contratos en línea.
6) *Coordinación.* Los comunicantes son capaces de coordinar sus acciones para la obtención de un bien común en presencia de potenciales usuarios hostiles.
7) *Nivel de colaboración*. En una comunicación entre varios usuarios, las propiedades del sistema se mantienen siempre que el número de adversarios no exceda de un cierto número.

## Clasificación de los sistemas criptográficos.

Podemos dividir los sistemas criptográficos según el tipo de transformación que realicen sobre el mensaje original en :

*Métodos de sustitución*. Sustituyen caracteres del mensaje original por otros de un alfabeto concertado previamente.

Definimos una sustitución de un alfabeto *A* en un alfabeto *B* como una aplicación biyectiva $\sigma$ tal que se reemplaza la letra $l$ por la letra $\sigma(l)$. Formalmente:

$$\sigma : A_m \rightarrow B_n \text{ con } n \geq m$$
$$\sigma : l \rightarrow \sigma(l)$$

En el caso en que *A* = *B* tenemos que el conjunto de todas las sustituciones en *A* forman un grupo simétrico. Si la cardinalidad del conjunto es *n*, el orden de grupo simétrico es *n*!

Sea *T* un texto en claro formado por los elementos $T = \{t_0, t_1, .., t_{n-1}\}$, *C* el conjunto de los elementos cifrados, y *k* una clave de sustitución formada por un conjunto de sustituciones $\sigma_i$ tales que $c_i = \sigma_i(t_i)$ con $0 \leq i < n$.

Los sistemas de sustitución se dividen a su vez en función del número de alfabetos que utilicen en:

*Sistemas monoalfabéticos*. Son sistemas en los cuales se sustituye un símbolo del alfabeto por otro. Formalmente, según la definición anterior, decimos que $E_k$ es una sustitución monoalfabética si $\sigma_i$ es la misma para cada *i*.

*Sistemas polialfabéticos*. Son sistemas en los que se utilizan varios alfabetos para la sustitución de los símbolos. Formalmente, decimos que $E_k$ es una sustitución polialfabética si los $\sigma_i$ son diferentes.

*Métodos de transposición*. Realizan el cifrado mediante la reordenación de los caracteres del alfabeto siguiendo un método dado.

Definimos una permutación $\pi$ como la reordenación de los elementos de un conjunto de forma que el elemento que se encuentra en la posición *i* pase a ocupar la posición $\pi(i)$. Es decir, $\pi$ define una aplicación de los elementos de un conjunto en sí mismo. Formalmente, sea *S* un conjunto de *n* elementos tal que $S = \{s_0, s_1, .., s_n\}$, tenemos que $\pi : S \rightarrow S$ con $\pi : s_i \rightarrow s_{\pi(i)}$ $0 \leq i < n$. El número de permutaciones diferentes de *n* elementos es *n*!

Según el número de claves que utilicen para el cifrado y descifrado de la información y la forma de gestionarlas en:

*Sistemas de Clave privada (simétricos).*

En estos sistemas el emisor y el receptor comparten una clave que es única y sirve tanto para cifrar como para descifrar. Estos sistemas son bastante utilizados pero tiene el problema de la distribución de claves. En un sistema con *n* usuarios serían necesarias $\frac{n(n-1)}{2}$ claves. Por otra parte para la distribución de claves es necesario un camino seguro.

Un ejemplo de sistema de este tipo es el DES, desarrollado por IBM en los años setenta, que fue adoptado por el NIST.

*Sistemas de clave pública (asimétricos).*

En estos sistemas se utilizan dos claves, una de cifrado que es pública y una de descifrado que es secreta. Con estos sistemas la gestión de claves es más sencilla. Para un sistema con *n* usuarios solo serían necesarias 2*n* claves. Tienen como desventaja el ser en general más costosos en tiempo de cifrado y descifrado que los anteriores.

*Sistemas de clave en deposito (key escrow).*

Una de las características requeridas de cualquier sistema de cifrado es el secreto. Esta cualidad en el caso de protección de datos legales, puede llegar a ser un serio contratiempo cuando se utiliza la criptografía para proteger datos ilegales. Desgraciadamente los delincuentes han empezado a hacer uso de técnicas criptográficas para proteger sus datos. Esto plantea un grave problema ético sobre que es más importante la privacidad o el bien común. Pasando por alto la ética, en Estados Unidos se ha producido una gran controversia por la intención de la Administración de obligar a todos los usuarios a utilizar métodos de cifrado que pudiesen ser descifrados en tiempo real por los organismos estatales autorizados a ello. Uno de los sistemas para conseguir esto son los sistemas de clave compartida (*key escrow*) fervientemente defendidos por Dorothy Denning entre otros. Estos sistemas se basan en la utilización de dos claves, una particular y una maestra que se entregará al departamento de la Administración correspondiente. Esta clave maestra permite, en ausencia de la clave privada, el descifrado del texto.

Estos métodos han suscitado gran controversia, ya que los usuarios no ven con buenos ojos el que la Administración pueda acceder a datos confidenciales, así como, tampoco se fían de la capacidad de la Administración para salvaguardar sus datos.

## Cifrado en bloque y cifrado en flujo.

Todos los métodos de cifrado enunciados anteriormente forman parte de uno de estos grupos. La diferencia básica entre ambos es la unidad básica de cifrado de la información. En un sistema de cifrado en flujo se cifra por separado cada una de los componentes básicos del mensaje, carácter a carácter o símbolo a símbolo, con lo cual solo podrán aplicarse al texto sustituciones al texto en claro. Es decir, sea *T* un texto en claro formado por los elementos $T = \{t_0, t_1, .., t_{n-1}\}$ pertenecientes a un alfabeto

$A = \{a_1,..,a_m\}$, el conjunto de los elementos cifrados con la clave *k* y el conjunto de sustituciones $\sigma_i$ se define como $c_i = \sigma_i(t_i)\,\text{con}\,0 \le i < n$ y $\sigma_i$ dependiendo generalmente de uno o varios de sus predecesores. La ventaja principal de los algoritmos de flujo es su velocidad y la posibilidad de cifrar, sin artificios, conjuntos de datos sin una estructura y un tamaño predefinidos.

Un sistema de cifrado en bloque, tal como su nombre indica, cifra los datos en bloques de tamaño fijo que son manipulados, bien por sustituciones, bien por transposiciones o bien por una combinación de ambos. La mayoría de los algoritmos comerciales son de este tipo al ser, en general, más seguros, y en el caso de los algoritmos de clave secreta lo suficientemente rápidos para la mayoría de las aplicaciones. Hay que hacer notar que, como veremos más adelante, un algoritmo de cifrado en bloque de clave secreta puede simular el funcionamiento de un algoritmo de cifrado en flujo poniéndolo a trabajar en modo CBC (Cipher Block Chaining).

## Concepto de secreto perfecto.

Un sistema de secreto perfecto necesita que el espacio de claves sea como mínimo igual al de mensajes. Formalmente:

Sean $M = \{m_1, m_2,.., m_n\}$ el conjunto de mensajes en claro, $C = \{c_1, c_2,.., c_x\}$ el conjunto de mensajes cifrados y $K = \{k_1, k_2,., k_y\}$ el conjunto de posibles claves. Se cumple además que $\sum_{i=1}^{n} p(m_i) = 1$, $\sum_{i=1}^{y} p(k_i) = 1$ y $\sum_{i=1}^{x} p(c_i) = 1$, se dice que un sistema cumple la condición de secreto perfecto si para cualquier *m* y *c* se cumple que *p(m/c)=p(m)* y por lo tanto *p(c/m)=p(c).*

*Teorema*. Sea *C* un sistema de cifrado tal que el número de mensajes, el número de claves y el de criptogramas es idéntico. Se dice que *C* tiene secreto perfecto si y solo si se cumple que:

a) Existe una transformación única *T* para cada mensaje a un criptograma.
b) Toda las claves son equiprobables.

Un sistema es destructible si conocida la suficiente cantidad de mensaje cifrado, se puede llegar a determinar la clave. La incertidumbre dada como la entropía de la clave con respecto al cifrado viene dada por:

$$H(K/C) = -\sum_{c} p(c) \sum_{k} p(k/c) \log_2 p(k/c)$$

Definimos como distancia de unicidad el número mínimo de caracteres cifrados necesarios para que la entropía anterior se aproxime a cero. En el caso de que esto no ocurra nunca se dice que el sistema es incondicionalmente seguro.

$$N = \frac{H(K)}{D}$$

El valor de *N* nos da la cantidad de caracteres cifrados necesarios para determinar la clave, sin embargo no nos da ninguna valoración del esfuerzo necesario para hacerlo. Los cifrados de uso único (*one time pad*) como el de Vernam se basan en que el tamaño de la clave sea como mínimo de el mismo que el del texto a cifrar, de esta manera $H(K) = \log_2(2^{RN}) = RN \log_2 2 = RN$, con lo cual $N = \frac{RN}{D}$.

El concepto de sistema incondicionalmente seguro, si bien es útil como resultado teórico, es impracticable en la realidad debido al esfuerzo requerido en el almacenamiento, gestión y coordinación en el manejo de las claves para sesión. En la realidad nos conformaremos con sistemas lo suficientemente seguros, entendiendo por esto, sistemas que cumplan las siguientes condiciones:

1) No existe un método para recuperar las claves que no sea la prueba exhaustiva.
2) El esfuerzo necesario para realizar esta prueba es técnica o económicamente inviable.

## Factor de trabajo.

Es el trabajo medio necesario para obtener la clave en función del número de caracteres interceptados. Evidentemente debe ser alto para evitar que el criptoanálisis sea factible. Sin embargo aunque el factor de trabajo sea alto, esto no es necesariamente un indicativo de que el criptoanálisis es inviable. El factor de trabajo mide el trabajo *medio*, el criptoanalista intentará encontrar una debilidad explotable que le permita reducir este factor.

## Confusión y difusión.

Estos conceptos introducidos por Shannon son la base de muchos de los cifrados modernos como el DES. El propósito de la difusión es enmascarar la redundancia del mensaje en claro distribuyéndola por todo el mensaje, de esta manera el posible espía necesitará acceder a más texto cifrado para obtener la clave mediante un ataque estadístico. Una de las formas de obtener difusión es mediante permutaciones. Un problema inherente a la difusión es el de la propagación de errores. Un error en la transmisión del criptograma puede conducir a muchos errores en el mensaje una vez descifrado.

La confusión pretende por su parte lograr que la relación entre mensaje, clave y cifrado sea lo más compleja posible, esto se logra haciendo que cualquier carácter del criptograma dependa virtualmente del conjunto de la clave. De esta manera se logra evitar la disminución del espacio de claves a examinar para determinar la clave real por parte de un potencial criptoanalista. Los sistemas de cifrado en flujo hacen uso de esta propiedad, evitando el principal problema de los cifrados en bloque que es la propagación de errores.

Los conceptos anteriores son la base de la mayoría de los algoritmos de cifrado actuales, en los cuales se aplican reiteradas sustituciones a la clave y permutaciones al mensaje de forma que cada bit del mensaje cifrado se obtenga de la clave y del mensaje en claro de una forma no lineal, pero invertible.

## Criterios de Shannon.

En los años cuarenta, Shannon sugirió los criterios básicos que debían cumplir los sistemas de cifrado modernos. Los puntos a tener en cuenta eran:

a) El sistema debe proporcionar suficiente secreto.
b) El tamaño de la clave debe ser lo suficientemente corto para ser sencillo de recordar y lo suficientemente largo para proveer de suficiente seguridad.

c) Las operaciones de cifrado y descifrado deben ser sencillas.
d) El sistema debe tener una baja propagación de errores.
e) El tamaño del mensaje no debe crecer.

En el momento en que Shannon dio estas indicaciones, el uso de dispositivos electrónicos capaces de realizar de forma automática el cifrado era muy raro, costoso y en general no disponible para el uso público. Los sistemas de cifrado eran manuales y para ello era muy importante la simplicidad de uso. Evidentemente con la aparición de los ordenadores alguno de estos puntos no es tan relevante como en su día. Sin embargo en su base siguen siendo conceptos totalmente válidos en la actualidad.

## Reglas de Kerchoffs.

Auguste Kerckhoffs Von Nieuwenhof (1835-1903), publicó en enero y febrero de 1883 en el *Journal des sciences militaires* sendos artículos con el titulo *La cryptographie Militaire*[KER83]. En estos artículos, se especifica claramente que la seguridad de un sistema estratégico se basa totalmente, o de forma esencial, en el secreto de la clave. Este aseveración es conocida popularmente como el principio de Kerckhoffs. Es decir debemos presuponer que el posible criptoanalista conoce la forma de cifrar y descifrar mensajes. Kerckhoffs enunció una serie de reglas que debía cumplir un buen sistema de cifrado. Estas reglas, adaptadas a la época actual, quedarían como*:

1) El sistema de cifrado debe ser impenetrable, sino en teoría, sí en la practica.
2) El hecho de que el sistema se vea comprometido no debe dañar a los corresponsales.
3) La clave debe ser fácil de memorizar y fácil de sustituir.
4) Los criptogramas deben ser adecuados para la transmisión por los medios habituales.
5) El aparato y los documentos de cifrado deben ser fáciles de transportar , es necesario que la operación de cifrado la realice una sola persona.
6) El sistema debe ser sencillo.
7) Todo sistema debe estar compuesta por dos tipos de información:
   - Publica
   - Privada.
8) La complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido.

* Las seis reglas tal como las publicó Kerckhoffs son las siguientes:
1) El sistema debe ser materialmente, si no matemáticamente, indescifrable.
2) Es necesario que no exija el secreto, y que pueda sin inconveniente caer en manos del enemigo.
3) La clave debe poder ser comunicada y retenida sin la ayuda de notas escritas, y ser cambiada o modificada a gusto de los corresponsales.
4) Debe ser aplicable a la correspondencia telegráfica.
5) Debe ser portátil, y que su manejo o funcionamiento no debe exigir el concurso de varias personas.
6) Por fin, es necesario, vistas las circunstancias que exige su aplicación, que el sistema sea de uso fácil, no requiriendo ni tensión de espíritu, ni el conocimiento de una larga serie de reglas a seguir.

## Características deseables de un sistema criptográfico.

En base a lo expuesto anteriormente podemos concluir una serie de propiedades deseables para cualquier sistema criptográfico:

a) *Factor de trabajo alto*. El sistema debe ser computacionalmente imposible de romper por un criptoanalista con los métodos conocidos.
b) *Tamaño pequeño de clave*. Una forma de compensar una cierta debilidad de un sistema es el cambio frecuente de la clave de cifrado. Si el tamaño de la clave es pequeño y es relativamente fácil generar claves seguras, ésta puede ser cambiada muy frecuentemente, con lo cual se gana en seguridad el sistema.
c) *Simplicidad*. Si bien esta cualidad es más necesaria cuando se trata de sistemas manuales, en determinados sistemas en los cuales la velocidad de cifrado es una limitación a tener en cuenta, la complejidad puede generar mayor lentitud en el cifrado y puede ser un grave inconveniente.
d) *Baja propagación de errores*. Algunos tipos de cifrado denominados encadenados utilizan el bloque de texto cifrado anteriormente para cifrar el texto siguiente. Esto añade complejidad al proceso de criptoanálisis, pero en el caso de producirse un error, éste se trasmitiría al resto del texto haciendo este indescifrable aunque se conozca la clave.

Así como el sistema debe cumplir una serie de reglas, el conjunto de usuarios que utilizan la criptografía como método para proteger sus datos deben de tener en cuenta a su vez una serie de reglas.

a) Ningún sistema, exceptuando el *one time pad*, es absolutamente seguro, debemos tener pues la convicción de que alguna vez será forzado.

b) La elección del sistema criptográfico debe estar en función de la vida útil de los datos a proteger. El sistema debe proteger los datos como mínimo hasta que estos hayan perdido su valor o este sea muy bajo. Esta regla es muy difusa y presupone un cierto conocimiento de la habilidad del posible criptoanalista. Debemos pues tomar una posición pesimista, siempre es mejor sobrevalorar las capacidades del posible interceptor de la información que infravalorarlas ya que puede darnos un falso sentimiento de seguridad en un sistema que puede ser totalmente inseguro.

c) Cuanto más se use un sistema, mayor será la probabilidad de que pueda ser forzado. Cuanto más se utiliza un sistema, existe un mayor flujo de información y por lo tanto una mayor probabilidad de que un criptoanalista puede obtener la suficiente cantidad de datos para analizar y como consecuencia poner en peligro el sistema.

d) Jamás debe enviarse, escribirse o almacenarse el texto cifrado y el original. En el caso de que sea necesario hacerlo, el original debe estar parafraseado para dificultar la labor de un potencial criptoanalista.

e) Los canales de comunicación deben ser seguros y deben ser utilizados de una forma periódica aunque no se transmita ningún dato útil. Esta medida nos permitirá reducir el peligro de obtención de información por análisis del trafico.

f) El conocimiento de los sistemas y métodos criptográficos debe estar restringido al personal autorizado para ello. Una adecuada separación de

funciones y responsabilidades sigue siendo el mejor sistema de control interno de la información.
g) Todos los sistemas, documentación e información sobre los mismos deben ser inventariados periódicamente.
h) La clave del sistema debe cambiarse periódicamente. Esta periodicidad es función del volumen de trafico y de la vida útil de los datos.
i) No enviar nunca el mismo mensaje cifrado en dos sistemas o claves diferentes.
j) El mensaje debe ser enviado totalmente cifrado, nunca parcialmente.
k) En el caso de sospecha de que el sistema haya sido forzado debe procederse al cambio inmediato de claves o si fuera necesario de sistema.

En el caso de no cumplirse alguna de las reglas el sistema se puede considerar inseguro y es en la explotación de la debilidad provocada por el incumplimiento de las mismas en las que tiene que basarse el criptoanalista. Bauer en [BAU82] hace una recopilación de las reglas que deben tenerse en cuenta en el trabajo criptográfico basadas en la experiencia de siglos de criptografía y de los trabajos escritos hasta el momento. La mayoría coinciden con las anteriores, sin embargo es interesante comprobar que aunque algunas de ellas tienen siglos, siguen siendo válidas hoy en día.

1) No subestimar al enemigo.
2) Solo el criptoanalista puede juzgar la seguridad de un método de cifrado.
3) Cuando se juzga la seguridad de un método criptográfico, uno tiene que asumir que el enemigo conoce el método (el sistema).
4) Complicaciones superficiales pueden ser ilusorias: pueden inducir a un sentimiento ilusorio de seguridad.
5) Cuando se juzga la seguridad de un método criptográfico, deben tenerse en cuenta los errores en el cifrado y otros fallos en la disciplina de cifrado.

## Seguridad teórica y computacional.

La seguridad teórica viene dada por el concepto de secreto perfecto definido por Shannon en sus trabajos tal como lo hemos definido anteriormente. Este postuló que un sistema de secreto perfecto es aquel en el que se cumple que la probabilidad de que dado un mensaje cifrado *c*, la probabilidad de que el mensaje en claro sea *m* es igual a la probabilidad de que el mensaje en claro sea *m* sin el conocimiento del texto cifrado.

Es decir que el conocimiento a priori no nos da ninguna información sobre el conocimiento a posteriori. Sin embargo el único método que se conoce que cumpla esta condición es el *one time pad*, en el cual la clave es tan larga como el mensaje a cifrar y además absolutamente aleatoria. Generalmente se ha considerado impracticable el uso de sistemas de este tipo, buscándose sistemas que sean computacionalmente seguros, es decir, que el costo de obtener el mensaje original sin conocer la clave es extremadamente alto en tiempo o en espacio de computación. Debemos tener en cuenta sin embargo que las posibilidades técnicas de hoy en día hacen que el uso de los sistemas basados en clave no reutilizable, sea una posibilidad a tener en cuenta. Tal como se indica en [FOS97], con un grabador de CD-ROM, un contador Geiger y un oscilador podrían generarse fácilmente un CD-ROM con claves extremadamente largas y absolutamente aleatorias.