Introducción:

Con el aumento del uso de las computadoras, el crecimiento explosivo de las redes de computadoras y el comercio electrónico, muchas computadoras hoy en día son conectadas a redes públicas no seguras, con lo que hay una gran porción de amenazas latentes referidas a esto.
La comunicación entre personas a través de redes de computadoras, hoy es común y por ahí, no se dimensionan los problemas a los que uno se expone al introducir información dentro de ellas.
Siempre que dos computadoras se comuniquen sobre canales no seguros, los datos que son transferidos pueden ser modificados o copiados con el objetivo de obtenerlos para algún fin determinado. Por eso los datos que son transferidos deben ser asegurados y la criptografía provee una parte para ayudar a esto.
Pero nos surge la pregunta; **¿Qué es la CRIPTOGRAFIA?**.
Según el Diccionario de la Real Academia, la palabra Criptografía viene del griego **Kryptos**, que significa oculto y **gráphein**, escritura, y su definición es : "*Arte de escribir con clave secreta o de un modo enigmático*". Obviamente la Criptografía hace años que dejo de ser un arte para convertirse en una técnica. O más bien un conglomerado de técnicas, que tratan sobre la protección - ocultamiento frente a observadores no autorizados - de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Teoría de Números que estudia las propiedades de los números enteros y la Complejidad Algorítmica.
Debemos notar que la palabra **Criptografía** sólo hace referencia al uso de códigos, por lo que no engloba a las técnicas que se usan para romper dichos códigos, conocidas en su conjunto como **Criptoanálisis**. En cualquier caso ambas disciplinas están íntimamente ligadas no olvidemos que cuando se diseña un sistema para cifrar información, hay que tener muy presente su posible criptoanálisis, ya que en caso contrario podríamos llevarnos desagradables sorpresas. Finalmente, el término **Criptología**, aunque no está aún en el Diccionario se emplea habitualmente para agrupar tanto a la Criptografía como al Criptoanálisis.
Bueno ya sabemos su significado, pero cual sería su objetivo brevemente?, su objetivo es proveer seguridad en las comunicaciones, es decir proteger la información que está siendo transmitida por algún medio que como dijimos se considera inseguro.
La criptografía *es* una herramienta, que sirve para ocultar información. Dentro de los usos más frecuentes, se encuentra el intercambio de mensajes, almacenado de password, ocultamiento de archivos.
Veamos un ejemplo simple, para tener un pantallaso general, así luego de a poco nos vamos metiendo en el tema: si alguien desea mandar información confidencial, aplica técnicas criptográficas para poder "esconder" el mensaje, a esta acción la llamamos encriptar, luego de esto, manda el mensaje por una línea de comunicación que se supone insegura y después sólo el receptor autorizado puede leer el mensaje escondido, la acción para poder leer el mensaje la llamamos desencriptar.

Al plantear el ejemplo anterior, nos surgen algunas preguntas, sobre el proceso criptográfico en general y cuales serían sus elementos básicos. Entonces...
El proceso criptográfico tiene los siguientes elementos básicos:

- La información inicial (el mensaje a enviar, por ejemplo), llamada texto plano.
- El algoritmo criptográfico.
- La información final (el mensaje encriptado), llamado texto cifrado.

El proceso consta de tomar el texto plano, aplicarle el algoritmo y la salida es el texto cifrado. Gráficamente:

Pero nos preguntamos ahora, luego de tener el texto cifrado, y enviarlo por la red el receptor lo recibe y como hace para obtener el texto plano. A ésta altura, diremos que vuelve aplicar el algoritmo al texto cifrado y obtiene el texto plano.
La entrada al algoritmo del texto plano /texto cifrado, no es la única, sino que también entra una clave, que dependiendo el tipo de sistema podrá ser la misma o no, para el encriptación y desencriptación. Existen variantes de cómo se realiza éste proceso, dependiendo el tipo de criptosistema que se utilice, pero más adelante, detallaremos.
Ahora definiremos algunos conceptos:

- Encriptación: es la transformación del texto planto en texto cifrado.
- Desencriptación: es la transformación del texto cifrado en texto plano.
- Algoritmo Criptográfico: es una función que convierte el texto plano en cifrado y viceversa.

Ampliando, el algoritmo criptográfico, es la combinación de funciones matemáticas de diferente grado de complejidad, éste factor puede influenciar en la elección del algoritmo, pues a mayor complejidad, mayor tiempo de procesamiento, lo que se ve reflejado en costo computacional (por ejemplo, tiempo, recursos utilizados.).

Algo de historia, objetivos y rol de la criptografía...

La criptografía desde sus inicios llegó a ser una herramienta muy usada en el ambiente militar. La criptografía actual, se inicia en la segunda mitad de la década de los años 70. No es hasta la invención del sistema conocido como **DES** (**D**ata **E**ncryption **S**tandard) en 1976 que se da a conocer mas ampliamente, principalmente en el mundo industrial y comercial. Posteriormente con el sistema **RSA** (**R**ivest, **S**hamir, **A**dleman) en 1978, se abre el comienzo de la criptografía en un gran rango de aplicaciones: en transmisiones militares, en transacciones financieras, en comunicación vía satélite, en redes de computadoras, en líneas telefónicas, en transmisiones de televisión etcétera.

Entendemos que la criptografía trata de dar seguridad en las comunicaciones en un sentido lógico, pero no podemos dejar de tener en cuenta que la seguridad de la información (confidencialidad, integridad, disponibilidad, uso legítimo, etc), no sólo se logra con esto, sino que tiene que trabajar junto con otras áreas de seguridad (física, de personal , administración, etc), para poder lograrla.
Hay muchas amenazas potenciales para los sistemas de información: penetración, violación de autorización, implantación de caballos de Troya , monitoreo en las comunicaciones, denegación de servicios y repudiación. Hay varios servicios de seguridad que deben ser implementados para proteger los sistemas de éstas amenazas: servicios de autenticación, servicios de control de acceso, servicios de confidencialidad, servicios de integridad de los datos, servicios de no repudiación.

Las técnicas criptográficas son importantes bloques de construcción en la implementación de servicios de seguridad. El bloque de construcción más básico, es el algoritmo de encripción usado. La confianza de éste depende exclusivamente de la clave para proteger los datos, pues el conocimiento del algoritmo, no está restringido. El algoritmo debe ser diseñado para resistir el criptoanálisis. Al momento de seleccionar uno, se puede acceder a las publicaciones de los análisis que le han realizado expertos, para poder detectar si tiene o no serias debilidades que podrían ser usadas por un atacante.

La tecnología está basada sobre la esencia de códigos secretos aumentados por matemáticas modernas que protegen los datos. Hay cosas que hacen el uso de la criptografía segura, es decir, viéndolo en un criptosistema, la fortaleza del mismo estará dada principalmente por los siguientes factores:

- Tipo y complejidad del algoritmo.
- Confidencialidad y longitud de la clave.
- Otro factor, es el tiempo estimado que se tarda en desencriptar mensajes de éste criptosistema, mediante los más modernos recursos computacionales.

Un problema adicional a los criptosistemas es el manejo de las claves, el cual a veces se minimiza, con lo que aumentan los riesgos. El problema se trata de la distribución, almacenamiento y caducidad(deshecho) de las claves, lo cual es una tarea que demanda una carga administrativa muy pesada.

Para poder entender un poco más la criptografía, plantearemos qué tipo de problemas resuelve, desde el punto de vista de las propiedades de la seguridad informática.

- **La privacidad o confidencialidad**: se refiere a que la información sólo pueda ser leída por personas autorizadas. Por ejemplo, en la comunicación por Internet es muy difícil estar seguros que la comunicación es privada, ya que no se tiene control de la línea de

comunicación. Por lo tanto al cifrar la información, cualquier intercepción no autorizada no podrá entender la información. Esto es posible si se usan técnicas criptográfica, en particular la privacidad se logra si se cifra el mensaje con un método simétrico.

- **La integridad**: se refiere a que la información no pueda ser alterada en el transcurso de ser enviada. Por ejemplo si realizamos una compra por Internet, se podrían modificar datos como el número de tarjeta de crédito o del pedido que podría traernos problemas. Esto puede ser solucionado con técnicas criptográficas con procesos simétricos o asimétricos. Lo que se intenta es que si se modificó /alteró algo en la información, si no pudo ser evitado, que pueda ser detectado.
- **La autenticidad**: se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba. Las técnicas necesarias para poder verificar la autenticidad tanto de personas como de mensajes usan quizá la más conocida aplicación de la criptografía asimétrica que es la firma digital, de algún modo ésta reemplaza a la firma autógrafa que se usa comúnmente. Para autenticar mensajes se usa criptografía simétrica.
- **El no rechazo o no repudiación**: se refiere a que no se pueda negar la autoría / recepción de un mensaje enviado / recibido.
- **La disponibilidad**: se refiere ha asegurar que a usuarios legítimos no le es denegado indebidamente el acceso a recursos e información, aquí no hay manera de asegurar que la información no se pierda, es el ASPECTO MÁS DEBIL.

Tipos de criptosistemas:

Aquí vamos a responder con exactitud, la pregunta que nos había planteado la introducción y que habíamos respondido rápidamente, dejándola abierta.
Cuando se diseña un sistema de seguridad, una gran cantidad de problemas pueden ser evitados si se puede comprobar autenticidad, garantizar privacidad, asegurar integridad y evitar el no rechazo.
La criptografía simétrica y asimétrica conjuntamente con otras técnicas, como el buen manejo de las claves y la legislación adecuada resuelven satisfactoriamente los problemas antes mencionados.

Existen dos tipos de criptosistemas según la clave:

- **De Clave Privada** (Simétricos)
- **De Clave Pública** (Asimétricos)
- **Irreversibles** cifran un texto no permitiendo su descifrado, una de sus utilizaciones es la del cifrado de las contraseñas, otra aplicación es la de las claves desechables o dinámicas que se utilizan en ciertos teléfonos móviles.

1.- Criptosistemas de Clave Privada:

Utiliza criptografía simétrica, la cual se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes, siempre y cuando anteriormente se hayan intercambiado la clave correspondiente, que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.
Para cada par de usuarios que intercambien mensajes existe una única clave que debe ser conocida por ambos y mantenida en secreto. La base de la seguridad de este sistema está dada por la protección de la clave, si se adivina la clave, el sistema queda expuesto a amenazas para aquellos mensajes que utilicen dicha clave.

Este tipo de criptografía se conoce también como criptografía de clave privada o criptografía de llave privada.

Existe una clasificación de este tipo de criptografía en tres familias, la cual se basa en el número de símbolos cifrados a la vez:

- la criptografía **simétrica de bloques** (block cipher), la cual toma el texto en claro y lo divide en bloques de igual longitud y cifra cada bloque independientemente. Suelen emplearse bloques de 64 bits
- la criptografía **simétrica de flujo** (stream cipher), en donde el texto en claro se cifra símbolo tras símbolo , cifrándose cada uno con clave diferente. Se utilizan donde se cuente con un ancho de banda restringido, además requiere independencia en los bloques transmitidos,
- la criptografía **simétrica de resumen** (hash functions).

Aunque con ligeras modificaciones un sistema de criptografía simétrica de bloques puede modificarse para convertirse en alguna de las otras dos formas, sin embargo es importante verlas por separado dado que se usan en diferentes aplicaciones.
La criptografía simétrica ha sido la más usada en toda la historia. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.
Aunque no existe un tipo de diseño estándar, quizá el más popular es el de Fiestel, que consiste esencialmente en aplicar un número finito de interacciones de cierta forma, que finalmente da como resultado el mensaje cifrado. Este es el caso del sistema criptográfico simétrico más conocido, **DES**.

Veamos cuales serían los pasos para poder comunicarnos:

I. Remitente y receptor se ponen de acuerdo en usar este sistema.
II. Remitente y receptor se ponen de acuerdo en la clave que van a usar.
III. Remitente encripta el mensaje con la clave elegida y se lo envía al receptor.
IV. Receptor recibe el mensaje enviado por el remitente y lo desencripta con la clave elegida.

Obs: los pasos I y II se realizan sólo una vez, cuando deseo tener forma de comunicarme con un usuario particular, luego cuando quiero enviar un mensaje este sólo se aplican los pasos III y IV.

De observar el sistema tenemos aspectos importantes de la seguridad:

- El intercambio de claves debe hacerse de manera que ninguna otra persona pueda llegar a conocerla. Esto llega a ser tan complejo que aparece el concepto de servidor de claves.
- Se basa en una confianza mutua, donde las partes involucradas, no comprometerán la privacidad de la clave (ie. La mantendrán en secreto).
- Este tipo de criptosistemas son en general más eficientes y mucho menos costosos computacionalmente que los criptosistemas de clave Pública.

2.- Criptosistemas de Clave Pública:

La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas. Diffie y Hellman, proponen una forma para hacer esto, sin embargo no fue hasta que el popular método de **R**ivest **S**hamir y **A**dleman **RSA** publicado en 1978, cuando toma forma la criptografía asimétrica, su funcionamiento esta basado en la imposibilidad computacional de factorizar números enteros grandes.

Actualmente la Criptografía asimétrica es muy usada, sus dos principales aplicaciones son el intercambio de claves privadas y la firma digital, una firma digital se puede definir como una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario. Los fundamentos de la criptografía asimétrica pertenecen a la teoría de números.

En la actualidad la criptografía asimétrica o de clave pública se divide en tres familias según el problema matemático del cual basan su seguridad:

- La primera familias la que basa su seguridad en el **P**roblema de **F**actorización **E**ntera **PFE**, los sistemas que pertenecen a esta familia son, el sistema **RSA**, y el de **R**abin **W**illiams **RW,**
- La segunda familia es la que basa su seguridad en el **P**roblema del **L**ogaritmo **D**iscreto **PLD**, a esta familia pertenece el sistema de **D**iffie **H**ellman **DH** de intercambio de claves y el sistema **DSA** de firma digital y
- La tercera familia es la que basa su seguridad en el **P**roblema del **L**ogaritmo **D**iscreto **E**líptico **PLDE**, en este caso hay varios esquemas tanto de intercambio de claves como de firma digital que

existen como el **DHE** (Diffie Hellman Elíptico), **DSAE**, (**N**yberg-**R**ueppel) **NRE**, (**M**enezes, **Q**u, **V**anstone) **MQV**, etcétera.

Aunque a las familias anteriores pertenecen los sistemas asimétricos más conocidos, existen otro tipo de sistemas que basan su seguridad en problemas diferentes como por ejemplo, en el Problema del Logaritmo Discreto Hiperelíptico, sobre problemas de retículas y sobre subconjuntos de clases de campos numéricos reales y complejos.

La base de la seguridad de este sistema está en la protección de la clave privada. No se puede utilizar la misma clave para encriptar que para desencriptar, lo que si se puede hacer es:

Encriptar	Desencriptar
Clave Pública	Clave Privada
Clave Privada	Clave Pública

Veamos cuales serían los pasos para poder comunicarnos:

I. Remitente y receptor se ponen de acuerdo en usar este sistema.
II. Remitente y receptor obtienen sus propias claves privadas e intercambian sus claves públicas.
III. Remitente encripta el mensaje con la clave pública del receptor y lo envía.
IV. Receptor recibe el mensaje enviado por el remitente y lo desencripta con la clave privada (nadie más puede desencriptar ya que sólo el receptor ***posee*** y ***conoce*** la clave privada).

Obs: los pasos I y II se realizan sólo una vez, cuando deseo tener forma de comunicarme con un usuario particular, luego cuando quiero enviar un mensaje este sólo se aplican los pasos III y IV. Además puede haber una variante en éstos pasos, ya que el remitente puede encriptar el mensaje con su clave privada, y cualquiera que conozca la clave pública puede desencriptarlo, generalmente se usa para mensajes no muy confidenciales y para tener la certeza de la identidad del remitente.

De observar el sistema tenemos aspectos importantes de la seguridad:

- Es más seguro que el de clave privada, pues no requiere el intercambio de las claves, en el sentido de que sólo viaja por el canal inseguro la clave pública, que sólo sirve para cifrar o para llevar a cabo la autenticación.
- Depende de la confianza mutua, pues se puede divulgar, el texto plano y texto cifrado y comprometer la clave privada (si fue encriptada con ésta). Además tiene que tener la característica de que el conocimiento de la clave pública no permita calcular la clave privada.
- Son mucho más costosos computacionalmente, por lo que se usan generalmente para codificar las claves simétricas (cortas).

Ataques...

Cualquier criptosistema está expuesto a ser atacado.
El objetivo de los ataques es revelar la información que se transmite. Ataca a la confidencialidad.
El criptoanálisis es el conjunto de métodos y técnicas usadas para obtener texto plano y /o la clave a partir de un texto cifrado sin la aplicación del algoritmo (que se supone conocido). El criptoanálisis fue ideado inicialmente para probar la fortaleza de un algoritmo, pero como toda herramienta que se usa para bien, puede usarse para otros objetivos no tan buenos, como es el de tratar de romper los sistemas criptográficos con fines oscuros.

Existen diferentes tipos de ataques a los criptosistemas:

- **Pasivos**: es la observación de la información que se transmite o que está en un archivo, para obtener sus datos para el criptoanálisis. El riesgo principal de este tipo de ataque es la divulgación del contenido del mensaje o archivo.
- **Activos**: son acciones que producen modificaciones en la información, pueden ser:
  - *Ataques a la autenticidad*: modificación del remitente o receptor del mensaje.
  - *Ataques a la integridad*: modifican el contenido del mensaje reorganizando el texto original o reemplazándolo por otro.

Las estrategias usadas por los ataques activos se pueden clasificar en:

Nombre	Objetivos y acciones
Por texto cifrado	Trata de obtener fragmento del texto cifrado para su posterior análisis para obtener el texto plano y si es posible la clave. Se basa en estudiar las características del texto cifrado. Hay herramientas y técnicas que le ayudan, ya que las variantes posibles hacen difícil hacer el análisis manualmente.
Por texto plano conocido	Se basa en deducir la clave a partir de texto plano / texto cifrado conocidos. Generalmente el texto plano es obtenido por un ataque al texto cifrado. Luego la clave es usada para desencriptar otros mensajes que se intercambien entre remitente y receptor.
Por texto plano elegido	Se basa en deducir la clave a partir de un texto cifrado conocido y un conjunto de texto plano que tienen alguna característica especial. Se aplica a sistemas simétricos
Por texto cifrado elegido	Se basa en deducir la clave a partir de un texto plano conocido y un conjunto de textos cifrados con algunos patrones particulares. Se aplica más a sistemas asimétricos.
Por clave elegida	Consiste en ir probando claves y analizar el texto plano resultante a partir de un texto cifrado conocido. Esta estrategia exige un cierto conocimiento de la estructura de la clave (longitud, etc). Es complementario a otros ataques.

Longitud de la clave.

Cuando dimos la introducción dijimos que una de las "entradas" al algoritmo, era la clave, y clasificamos los criptosistemas según se use la misma clave o no para encriptar y desencriptar. Sobre la longitud de la clave existe una gran discusión.
La elección de la longitud de la clave está controlado por el producto que se dispone para el uso. Pero a veces la decisión más importante es cuándo un producto tienen la longitud de clave suficiente para proteger la información.
También hay confusión, que viene provocada, pues diferentes técnicas combinan el uso de distintos tipos de claves. Un ejemplo de esto es el SSL es un protocolo de comunicación que proporciona principalmente tres servicios básicos de seguridad: confidencialidad, autenticación e integridad . Con el fin de garantizar dichos servicios, SSL hace uso tanto de la criptografía asimétrica (basada en la existencia de un par de claves, la pública y la privada) como de la criptografía simétrica (basada en la utilización de una única clave secreta). La justificación de dicha combinación viene dada por cuestiones de eficiencia, puesto que las transformaciones criptográficas (operaciones de cifrado y descifrado) realizadas mediante técnicas de criptografía asimétrica son del orden de diez mil veces más lentas que las realizadas con criptografía simétrica. SSL negocia en una primera fase utilizando criptografía asimétrica (por ejemplo RSA), y cifra posteriormente la comunicación utilizando criptografía simétrica (RC4, RC5, IDEA...).
La confusión es lógica, pero puede evitarse fácilmente identificando los principales algoritmos criptográficos y ubicándolos dentro de su categoría (simétricos o asimétricos).

Las claves empleadas en criptografía asimétrica tienen justificación matemática, mientras que las que se utilizan en criptografía simétrica suelen ser simples cadenas de bytes aleatorios. Esta diferencia de contenido hace que no sea comparable el tamaño de las claves simétricas y asimétricas.

Sobre el tamaño de las claves que es apropiado para brindarnos un nivel de seguridad aceptable, nos vamos a extender un poquito más y ha analizar algunos aspectos.
Se cree que a mayor tamaño de la clave es mayor el nivel de seguridad que nos proporciona, pero esto no es tan así, pues depende de la aplicación y de la cantidad de entropía en la clave. Bueno, pero qué es entropía, la entropía es una medida de la incertidumbre, cuanto más incierto es algo más entropía hay en ello, por eso hay que analizar dos factores importantes que pueden debilitar la entropía de las claves:

- **La primera es la calidad del algoritmo de cifrado**, pues si hay defectos en el algoritmo, reduce la entropía de las claves.
- **El origen de las claves**. Pueden ser derivadas de contraseñas, con todas las debilidades de éstas o derivadas aleatoriamente, lo cual no indica que son mejores. Existen soluciones para esto pero requiere de compromiso en el diseño.

Por ejemplo Microsoft presume de cifrado de 128 bits y basan su clave en la contraseña, con lo que se obtiene una clave con una entropía mucho pero mucho menor.

Viendo cada uno de los sistemas, el tamaño de clave simétrica suele oscilar entre los 40 y los 128 bits. Las claves de 40 bits, como las utilizadas por Netscape en su versión de exportación, pueden romperse en cuestión de horas, mientras que las claves de 128 bits son irrompibles actualmente. Otros tamaños estándar de clave son 56 bits (DES), que tampoco proporciona seguridad hoy en día, ya que puede romperse en cuestión de días. La seguridad completa sólo se consigue actualmente utilizando claves no inferiores a 80 bits.
Por otro lado, el tamaño de clave asimétrica oscila entre los 512 bits y los 4096 bits. Las claves de 512 bits, también utilizadas por Netscape en su versión de exportación, han dejado de considerarse seguras últimamente, y no se recomienda el uso de claves inferiores a 1200 bits.
Sobre las recomendaciones de la cantidad mínima de bits para la clave, no es caprichosa, se tienen en cuenta los distintos tipos de ataques que pueden sufrir los distintos sistemas y quienes lo realizan, pero las cifras dadas pueden ser bajadas un poco dependiendo de la empresa que se esté hablando (en el sentido si le interesan a grandes corporaciones o no su información por ejemplo).

Luego de ataques y la longitud de claves...

Después de haber analizados los ataques y las longitudes de las claves, no podría surgir el siguiente interrogante:

Quién es el enemigo?, cual es el esfuerzo que éste dispondrá para atacarnos y entonces cuales son en realidad la longitud de clave que necesito para proteger mi sistema y por cuanto tiempo lo hará dicha clave.

Bueno para responder al interrogante, primero diríamos que hay tantos enemigos como podamos imaginarnos, y para saber de que son capaces podríamos clasificarlos en cuatro grupos según, el tiempo que dediquen a atacarnos y con los recursos que cuentan para esto. La clasificación es la siguiente:

Nombre	Características
Ataque Pirata	Es aquel efectuado por la típica persona de la informática que tiene a su disposición un par de computadoras para hacer con ellas lo que quiera.
Ataque Corsario	Es un atacante con mayores recursos, como una red de computadoras o computadoras especialmente construidas para reventar claves. Este tipo de ataque requiere un esfuerzo organizado y costoso.
Ataque mafioso	Es un ataque, con un esfuerzo como el corsario, pero a mayor nivel, hecho por un atacante con grandes recursos.
Ataque MIB	Es un atacante definitivo, con fondos ilimitados en material y dinero. MIB, es la abreviatura de Hombres de Negro.

Ahora podemos ver que en la mayoría de los algoritmos que utilizan clave simétrica, no hay un ataque criptoanalítico digno de ese nombre, es decir, no hay atajos. Eso significa que no hay más remedio que probar todas las posibles claves en busca de la correcta. La situación es mucho más compleja en criptografía asimétrica, pues cada algoritmo es diferente a los demás y exige un tratamiento especial, ya que su fundamento esta basado en teoría de grandes números.
Luego de hacer cuentas exhaustivas, razonamientos matemáticos y teniendo en cuenta las característica de cada uno de los tipos de ataques podemos concluir que:

Tipo clave	Pirata	Corsario	Mafioso	MIB
Clave simétrica	51 bits	64 bits	71 bits	77 bits
Clave asimétrica	518 bits	792 bits	956 bits	1138 bits

Luego podemos ver que el mínimo sería, para clave simétrica de 80 bits y para clave asimétrica de 1200 bits, pero aún no hemos respondido por completo el interrogante, pues por cuánto tiempo, no servirían

éstas claves, para esto deberemos analizar factores y predecir, y como toda predicción no se sabe si es correcta, pero vamos a tratar de hacerla lo mejor posible.
Los factores que nos van a afectar principalmente son:

- **Es el creciente aumento de la velocidad de cálculo**, la cual se ha regido por la ley de Moore, donde los procesadores duplican su velocidad cada 18 meses. Supondremos que ésta ley se mantendrá, con lo cual la capacidad de cálculo de los atacantes aumentará en un 59% anual, lo que significa que la longitud de las claves simétricas habrá de aumentar en dos bits cada tres años para mantener el mismo nivel de seguridad. Para las claves asimétricas, habrá un aumento aunque no lineal.
- **El aumento de presupuesto**, con lo que se tendrá un crecimiento anual en los medios disponibles de un 7% aproximadamente, que combinando con la ley de Moore, da un crecimiento de los medios de un 70%, que significa poder atacar claves de un bit más cada 16 meses más o menos (y cada 18 meses sin aumento de presupuesto). Pero en lo que respecta a claves asimétricas, se influenciado por un tercer aspecto que es el **aumento en la eficiencia de los algoritmos de factorización**. Luego con los avances en nuevos métodos criptoanalíticos para atacar sistemas de clave asimétrica han permitido que la potencia de dichos ataques se duplique cada 18 meses

Combinando ambos factores, los ataques contra sistemas simétricos aumenta un 70% por año, en el caso de los sistemas asimétricos el aumento es de 170%, lo que significa que las claves asimétricas se hacen más vulnerables con el paso del tiempo a mayor velocidad que las simétricas.
Lo que obtenemos al analizar teniendo en cuenta los factores antes mencionados son:

	Clave asimétrica (bits)				Clave simétrica (bits)			
Año	Pirata	Corsario	Mafioso	MIB	Pirata	Corsario	Mafioso	MIB
2000	518	792	956	1138	51	64	71	77
2005	657	970	1154	1357	55	68	75	81
2010	817	1169	1375	1599	59	72	79	85
2015	997	1391	1618	1866	62	76	82	89
2020	1200	1637	1886	2158	66	80	86	93
2025	1425	1907	2108	2476	70	83	90	97
2030	1675	20203	2500	2821	74	87	94	100
2035	1949	2524	2847	3193	78	91	98	104
2040	2248	2873	3221	3594	82	95	102	108
2045	2574	3250	3624	4024	85	99	105	112
2050	2926	3655	4056	4484	89	103	109	116

Luego de hacer todas estas predicciones podemos decir que hay demasiadas suposiciones, como:

- no se ha descubierto ningún tipo de ataque criptoanalítico de importancia en los algoritmos de clave simétrica más que el de la fuerza bruta, pero esto no está probado.
- No sabemos que forma tomarán los nuevos avances en la factorización de números primos, (base de la fortaleza de RSA).
- Suponemos que la factorización de números primos es la única manera práctica de violentar el algoritmos RSA, pero no está demostrado que sea la única manera y no sabemos si hay un camino más fácil. Además suponemos que el algoritmo Diffie-Hellman es tan resistente como RSA para claves similares pero no ha sido demostrado.
- No sabemos si la ley de Moore se mantendrá.
- Además de menospreciar consideraciones de memoria entre otras cosas.

Luego todo es una incertidumbre.

Manejo de claves.

En General...

En cualquier sistema de cifrado es imprescindible llevar un control de las claves utilizadas, estableciendo una serie de procedimientos y normas para su distribución, almacenamiento y selección, que variará notablemente en función del sistema de cifrado empleado, privado o público.

El gran número de claves en un sistema de clave privada hace que la gestión sea mucho más compleja, tanto los procedimientos de distribución, como los de almacenamiento, en comparación con el número necesario en un sistema de clave pública, donde cada usuario sólo debe mantener una clave.

Cuando se trabaja con varias claves de pequeño tamaño es posible memorizarlas sin necesidad de recurrir a ningún sistema para su almacenamiento, pero cuando se deben utilizar diversas claves para cifrar información y acceder a diferentes sistemas, se hace imprescindible su almacenamiento.

En los sistemas de clave pública, el problema del almacenamiento está resuelto puesto que el usuario sólo debe mantener su clave privada, estando la clave pública en una base de datos o directorio de claves públicas que alguien se encarga de mantener. Estos directorios, que contienen la identidad de los usuarios y sus claves, así como otros datos referentes a los usuarios y claves incluyen firmas digitales para su certificación.

En los sistemas de clave privada es en donde surgen los problemas, principalmente por el número de claves que se deben gestionar. Hay varias soluciones a este problema. La más simple es almacenar todas las claves de un usuario o las comunes a un grupo de usuarios en un fichero cifrado. Para extraer cualquier clave no habría más que conocer la clave de cifrado del fichero o clave maestra que daría acceso a todas las demás. También se podría establecer una estructura jerárquica donde determinados usuarios puedan extraer sólo ciertas claves, existiendo también una clave maestra que daría acceso a todas las claves contenidas.

Para la distribución de claves en sistemas de clave privada también se puede emplear un sistema de clave pública, tal como el algoritmo de Diffie-Hellman, para intercambio de claves.

A la hora de elegir una clave, ya sea para cifrado de información, como de acceso a un sistema, debe evitarse la utilización de claves sencillas de descubrir y que puedan hacer inútil el sistema de cifrado más avanzado.

Es necesario llegar a un compromiso entre facilidad para recordar una clave y dificultad de que alguien la descubra. La utilización de algoritmos para obtener las claves soluciona el problema de la mala elección de estas por parte de los usuarios, aunque producirán claves difíciles de recordar. Existen diversos algoritmos de uso extendido para la generación de claves basados en operaciones como desplazamientos, rotaciones o permutaciones, y también es común la simple generación aleatoria. Por lo que la selección de una u otra forma tiene que estar de acuerdo con el sistema, tipo de organización y también con la aplicación que se le va a dar (ie. el tipo de información que está protegiendo), entre otras cosas.

Además las claves deben tener un tiempo de vida limitado , al menos por dos razones:

- Criptoanálisis.
- Si la clave por alguna razón puede ser comprometida o criptoanalizada, limitando el tiempo de vida, se limita el daño que puede ocurrir.

Más en profundidad: manejo de claves por medio de Certificados Digitales

Todos los criptosistemas, igualmente los de clave pública, dependen sobre algunas claves que deber ser secretas, por lo que se debe contar con un sistema seguro y eficiente para la generación, registración, backup y recuperación, distribución, actualización y revocación, tanto como la terminación. En general, la protección de las claves necesita ser realizada a través de todo su tiempo de vida.

Todas las claves secretas necesitan ser protegidas por propósitos de integridad y confidencialidad. Si es posible de ser almacenadas en un lugar físico seguro. Hay al menos dos formas de distribuir claves públicas:

- Manualmente.
- Certificados de claves públicas, son un interesante concepto técnico. Son una estructura de datos que identifica el propietario de una clave pública particular.

El certificado es un bloque de datos firmado digitalmente que contiene una clave pública y el nombre del usuario de la clave. El certificado declara que una entidad particular con un nombre particular posee una clave pública particular. La firma digital del certificado, es producido por una autoridad de certificación (CA).

Los certificados digitales, tienen una similitud con las licencias de conducir. El certificado digital da identidad a una clave pública y se comporta como una persona en el espacio cibernético. La idea es que una tercera entidad intervenga en la administración de las claves públicas y asegure que las claves públicas

tengan asociado un usuario claramente identificado (Esto fue inicialmente planteado por Kohnfelder del MIT en sus tesis de licenciatura).

Las partes más importantes de un certificado digital son:

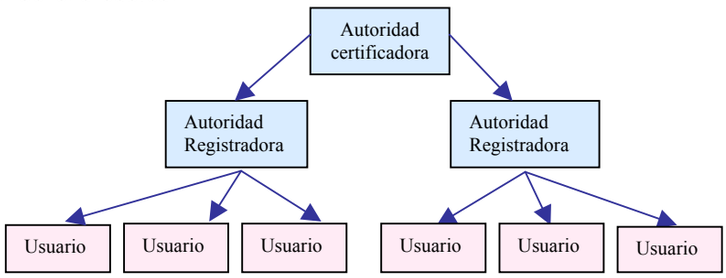
- Una clave pública
- La identidad del implicado: nombre y datos generales
- La firma privada de una tercera entidad llamada autoridad certificadora que todos conocen como tal y que validad la asociación de la clave pública en cuestión con la persona que dice ser.

CA. Autoridades de Certificación:

Una tarea central de una CA es la de autenticar la propiedad y las características de una clave pública, así esta puede ser confiable. Una vez que la CA certifica la propiedad y características son correctas, un certificado es distribuido / entregado, conteniendo la clave y otros detalles. El certificado es firmado digitalmente por el CA con su clave privada.

Existen varios tipos de certificados, la clave pública del CA, puede ser firmado por otro CA, llevando a una certificación jerárquica. Esto posibilita tener la clave pública certificada por diferentes CA´s. Otra posibilidad sería tener una sola CA, llevando a una certificación centralizada, pero este sistema es inflexible, aunque simple.

Veamos una estructura básica:



El papel de la Autoridad certificadora (**AC**) es de firmar los certificados digitales de los usuarios, generar los certificados, mantener el status correcto de los certificados, esto cumple el siguiente ciclo:

1) La generación del certificado se hace primero por una solicitud de un usuario, el usuario genera sus claves pública y privada y manda junto con los requerimientos de la solicitud su clave pública para que esta sea certificada por la **AC**.
2) Una vez que la **AR** (es la **AC** regional) verifica la autenticidad del usuario, la **AC** vía la **AR** firma el certificado digital y este es mandado al usuario
3) El status del usuario puede estar en: activo, inactivo o revocado. Si es activo el usuario puede hacer uso del certificado digital durante todo su periodo válido
4) Cuando termina el período de activación del certificado el usuario puede solicitar su renovación.

El usuario dueño de un certificado digital tiene la potencialidad de poder autentificarse con cualquier otra entidad usuaria, también puede intercambiar información de forma confidencial y estar seguro de que esta es integra, así los contactos vía el certificado digital no serán rechazados. Los primeros usuarios de certificados digitales fueron los servidores, actualmente son quienes más los usan, sin embargo también se ha incrementado el número de personas que los usan.

Casi no existe legislación acerca de las acciones y responsabilidades de los CA y los que poseen certificación. Muchas de las CA existentes son distribuidas como el resultado del establecimiento de sentencias de práctica de certificación. Estas sentencias son referidas para tener un acuerdo y estado claro de responsabilidades de los propietarios de certificados. Estas sentencias no sólo protege a la CA, sino que también informa, acerca de las políticas de la CA y como están implementadas. Estas políticas son un conjunto de reglas que un CA aplica en la distribución, administración y revocación de certificados, además de procedimientos operativos y aspectos de autenticación, requerimientos para diferentes niveles de clases de certificados, medios operativos, estándares, aplicaciones soportadas, practicas seguras, responsabilidades y obligaciones del CA y del poseedor del certificado, etc.

Entre las distintas responsabilidades y operaciones que pueden realizar encontramos las siguientes según de quién se trate: Las operaciones que pudiera realizar una **AC** están: Generar certificados, Revocar

certificados, Suspender certificados, Renovar certificados, Mantener un respaldo de certificados…..Las que pudiera realizar una **AR** están: Recibir las solicitudes de certificación, Proceso de la autenticación de usuarios, Generar las claves, Respaldo de las claves, Proceso de Recobrar las claves, Reportar las revocaciones….Y las actividades de los **usuarios**: Solicitar el certificado, Solicitar la revocación del certificado, Solicitar la renovación del certificado….

Distribución de Certificados.

Hay al menos dos conjuntos de protocolos que automáticamente derivan certificados de claves públicas:

- **Protocolo directorios**: por ejemplo X.500, tiene una tecnología compleja y el servicio provisto no tiene consigo el concepto de interconexión de sus directorios on-line, lo cual es dado por sus competidores LDAP (protocolo de Acceso Ligero a Internet), el cual es mucho más simple y fácil de implementar. Constituye un protocolo estándar útil para acceso de información almacenada en directorios, incluyendo el acceso almacenado de certificados de claves públicas.

- **Protocolo de intercambio de claves**: por ejemplo ANSI X9.17. Se ven en IPSEC y parte importante de SSL.

Mientras que la distribución de certificación transparente es usualmente mejor, no es la única forma. Muchos sistemas usan otros mecanismos para distribuir certificados interactivamente.

Revocación de Certificados

Un certificado de clave pública tiene un tiempo limitado de validez, indicado por el tiempo de comienzo y tiempo de expiración, los cuales son incluidos dentro de la parte firmada del certificado. La longitud de tiempo depende de la política utilizada.

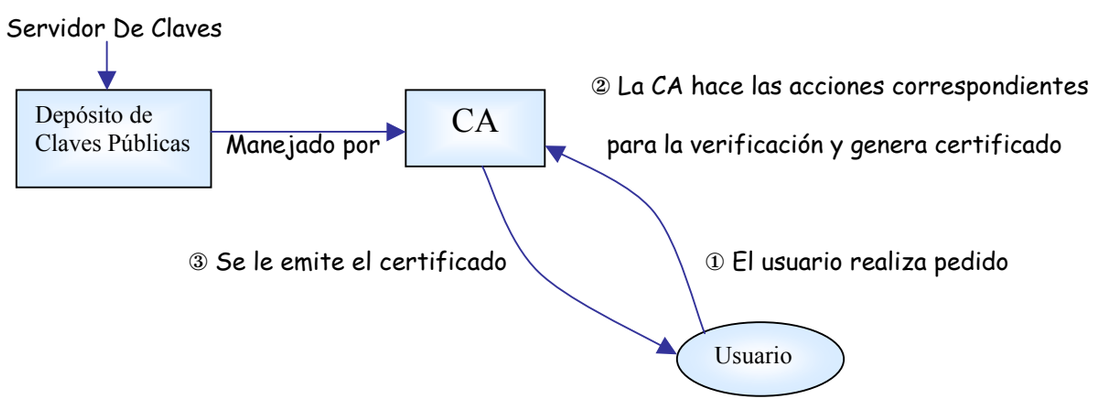
Sin embargo bajo algunas circunstancias el certificado puede ser revocado antes de que llegue a su tiempo de expiración, tales circunstancias son:

- Detección o suposición de compromiso de la correspondiente clave privada.
- Cambio de nombre
- Cambio de relación entre sujeto y autoridad de certificación.

Quién toma la decisión de revocar es la CA y luego deberá informarlo. Una forma es mediante una publicación de una lista de revocación de certificados (CRL) , pero cada cuánto y cómo es variante pues no hay un consenso y depende de la política.

En la práctica, el estado de un certificado cambia frecuentemente y, como cada vez que se piensa realizar una comunicación, es necesario validar el certificado, se debería consultar la CRL y de no estar, se puede iniciar la comunicación. El manejo de las listas de certificados revocados ha llegado a tener un gran costo sin embargo, aún no se ha reemplazado por otra técnica a pesar que se han propuesto ya salidas al problema.

Gráficamente todo el proceso podría verse como lo siguiente, teniendo en cuenta que puede haber una jerarquía de CA que no será representada por simplicidad del dibujo.



Tipos de Cifrados.

Bueno hemos vistos distintos tipos de sistemas, hablado de sus claves y sus características deseables, sabemos que el algoritmo es público, pero que es lo que hace para cifrar?. Para poder responder veamos cuales son los tipos de cifrado que podemos encontrar:

- **Trasposición o Permutación**, no sustituye los símbolos exclusivamente cambia el orden de los mismos, el cual produce un efecto de confusión.
- **Substitución**, Sustituye unos símbolos por otros, ejemplo método César, el cual produce un efecto de difusión.
- **Producto (Supercifrado ó Recifrados):** Son los cifrados obtenidos aplicando 2 o más veces los métodos anteriores, cuantos más métodos se apliquen más seguridad se tiene, siendo este método el más aplicado en la actualidad.

Las claves son usadas por los algoritmos para encriptar y desencriptar, sirven para controlar las trasposiciones y substituciones muy complejas.

Clasificación de los Algoritmos según su clave:

Podemos encontrar los siguientes tipos:

Algoritmos Simétricos	
Nombre	Descripción breve
DES (Data Ecription Standard)	Es un algoritmo diseñado por IBM y utilizado habitualmente desde los años 70. Es un método de cifrado altamente resistente frente a ataques criptoanalíticos diferenciales. Por desgracia, su tamaño de clave (56 bits) la hace vulnerable a ataques de fuerza bruta. En la actualidad ofrece protección contra el pirata informático habitual, pero no contra un esfuerzo masivo por parte de un usuario con grandes recursos, para estos hay que usar claves mayores. Es un algoritmo de cifrado por bloques.
Blowfich	Blowfish es un algoritmo desarrolló por Bruce Schneier. Es un cifrado por bloque con un tamaño 64-bits por bloque y longitud variable de la clave (hasta 448 bits). Ha ganado una cantidad justa de aceptación en varias aplicaciones. No se sabe de ningún ataque contra él.
CAST (Carlisle Adams y Stafford Tavares)	Tiene estructura similar a la de Blowfish. Parece ser un buen algoritmo, aunque tampoco lleva el tiempo suficiente como para haber sido atacado hasta la saciedad. De momento, sus posibilidades son buenas. Se conocen ataques criptoanalíticos contra la versión de clave 64 bits, aunque distan mucho de ser eficaces (requieren 2^17 textos sin cifrar y 2^48 cálculos diferentes). No se conocen ataques contra la versión de 128 bits. Ha sido patentado por Entrust Technologies, quienes permiten el uso libre de este algoritmo.
IDEA (International Data Encription Algorithm)	Ha sido desarrollado por Xuejia Lay y James Massey. A pesar de que solamente lleva unos años en uso, es probablemente el mejor algoritmo de bloques existente. Utiliza clave de 128 bits y se cree que es resistente al criptoanálisis. Se encuentra bajo patente de Ascom-Tech, aunque se permite su uso gratuito para aplicaciones no comerciales.
RC2	Es un código protegido bajo secreto comercial (aunque no patentado) por RSA Data Security Inc. Existen ataques criptoanalíticos que, aunque requieren de gran cantidad de texto cifrado, muestran las vulnerabilidades de RC-2. Existen versiones mejoradas, y hoy día RC2 tiende a utilizarse cada vez menos en beneficio de su "hermano mayor" RC4.
RC4	Es un intento de reemplazar RC2 por un algoritmo más sólido. También es un secreto comercial, aunque (al igual que RC2) su código fuente ha sido publicado en grupos de discusión. No se conocen ataques contra él. Forma una parte vital del sistema de cifrado en capas SSL, ampliamente utilizado en navegadores de Internet tales como Netscape Navigator y Microsoft Internet Explorer. Por desgracia, la versión exportable de RC4 tiene una clave de solamente 40 bits, lo que lo hace altamente vulnerable a ataques de fuerza bruta. La versión EEUU, con clave de 128 bits, es segura. Es un algoritmo cifrador de Flujo.

RC5	Fue diseñado por Ron Rivest y se encuentra bajo patente de RSA Data Security Inc. Es relativamente nuevo, y se conocen ciertos tipos de ataques contra él. Asimismo existe un cierto número (pequeño) de claves débiles que no deben utilizarse. A pesar de ello, se le considera un sistema seguro.
SAFER	Es un algoritmo diseñado por Robert Massey (uno de los creadores de IDEA). Tiene claves de hasta 128 bits y, a pesar de algunas debilidades en la primera versión y de ciertos ataques, parece un algoritmo seguro. Este programa fue desarrollado para la empresa Cylink, que algunos ligan a la no muy querida Agencia de Seguridad Nacional norteamericana (NSA); por ello, hay quien no se fía.
MD5 (Message Digest Algorithm 5)	Es un algoritmo seguro desarrollado por RSA Data Security, Inc. El MD5 no sirve para cifrar un mensaje ya que lo destruye completamente, el MD5 (o su hermano menor el MD2 o el MD4) "cifran" una entrada de forma irreversible, la información no es recuperable de ninguna manera ya que hay perdida de información.
SHA (Secure Hash Algorithm)	También SHS, Seguridad Hash Estándar: Este es un algoritmo de criptografía hash publicado por el Gobierno de los Estados Unidos. Produce valores hash a 160 bits de longitud arbitraria de cadena. Muchas personas lo consideran bastante bueno. Es un algoritmo bastante nuevo.
Rimpemd-160	Es el algoritmo hash más reciente, que se diseñó para reemplazar a MD4 y MD5. Produce un compendio de 20 bytes, según informes recibidos corre a 40 Mb/s en un 90 MHz Pentium y se ha puesto en el dominio público por su diseñadores.

Algoritmos Asimétricos	
Nombre	Descripción breve
RSA (Rivest, Shamir, Adleman)	Es el algoritmo de clave pública más utilizado, y uno de los más populares. En principio utiliza claves de cualquier longitud; en la actualidad se emplean claves de 1024 bits, consideradas lo bastante largas como para resistir ataques de fuerza bruta. Su seguridad se basa en la dificultad de factorizar números primos de gran tamaño. En principio se puede deducir la clave secreta conocida la clave pública, pero solamente por medio de la factorización de números de gran longitud (centenares de cifras). Está patentado en EEUU hasta el año 2000; es de uso libre en el resto del mundo. Es vulnerable a ciertos ataques (un atacante puede deducir la clave secreta si consigue que el creador de dicha clave "firme" digitalmente textos cuidadosamente elegidos), pero si se utiliza adecuadamente es un algoritmo seguro. Un detalle, no obstante, debe tenerse en cuenta. La dificultad intrínseca de factorizar grandes números es un tema abierto. Actualmente el método de factorización más rápido conocido es la Criba Numérica Especial de Campo (Special Number Field Sieve), pero *no está demostrado* que no haya otro mejor. Si se descubre un método de tiempo polinómico (esto es, cuyo tiempo de ejecución dependa del número N de cifras como N^a), cualquier producto de números primos podrá factorizarse con relativa facilidad. Es un tema sin resolver dentro de la llamada teoría de la complejidad. Mientras tanto, no obstante, todo parece indicar que el algoritmo RSA continuará siendo poco menos que invulnerable.
Diffie-Hellman	Es un algoritmo de intercambio de claves. Una variante conocida como El Gamal funciona como algoritmo de clave pública; por abuso del lenguaje, se suele conocer dicho algoritmo como Diffie-Hellman (o DH, variante ElGamal). Se basa en llamado problema de los logaritmos discretos, que se cree es computacionalmente tan complejo como el de la factorización de números primos (y, al igual que su primo RSA, *no está demostrado* que el problema de logaritmos discretos no se pueda resolver mediante herramientas matemáticas más poderosas en el futuro). Está siendo utilizado cada vez con más frecuencia, entre otras cosas por cuestiones de patentes (la patente D-H ha expirado). Aunque el algoritmo DH es más antiguo que el RSA, es más reciente en su utilización. Se ignora si suplantará a RSA o coexistirán.

De Curva Elíptica	Son los más recientes dentro del campo de los sistemas de clave pública. En general se creen que son bastante seguros, pero no ha sido demostrado. Existe un tipo de curvas que recientemente se ha revelado extremadamente vulnerable, por lo que éstas no deben usarse en criptografía. Existen muchos otros tipos de curvas, pero han de ser cuidadosamente examinadas para comprobar su idoneidad como base para un código de cifrado de datos. La valía de los sistemas de curvas elípticas permanece hoy por hoy bajo dudas.

Conclusión:

En un modelo criptográfico típico tenemos dos puntos a y b que se consideran *fiables* y se transmite información entre ellos a través de un canal *no fiable*. La criptografía se preocupa de los problemas de *transmisión confidencial y segura por el medio no fiable*, en tanto la seguridad informática se ocupa de asegurar la fiabilidad de los nodos a y b

La seguridad incondicional se produce cuando se conoce un mensaje cifrado c y *no es posible por ningún medio* conocer el mensaje original m a partir de este. La seguridad computacional significa que, aunque es teóricamente posible deducir m a partir de c, la capacidad en tiempo, proceso y recursos económicos para obtener este resultado es, *en la práctica, inalcanzable*. La seguridad incondicional es un concepto matemático y por lo tanto absoluto, la seguridad computacional es *muy relativa* ya que depende de la tecnología del momento, de los avances del criptoanálisis, etc. Los sistemas de encriptación usados en la práctica ofrecen solo *seguridad computacional*

En los sistemas abiertos (Internet por ejemplo) los algoritmos no deben ser secretos, así la seguridad del criptograma depende fundamentalmente de las claves empleadas. La fortaleza de los sistemas de clave privada es que resulta imposible calcular la clave k a partir del mensaje cifrado c. En los sistemas de clave pública su fortaleza descansa en la imposibilidad computacional de obtener la clave privada a partir de la clave pública.

El fundamento matemático de los criptosistemas se basa en la teoría de la información (C. Shannon), la teoría de los números y la teoría de la complejidad de los algoritmos. La teoría de la información se ocupa de la entropía de los mensajes (el porcentaje de información y redundancia que contienen). La teoría de los números trata sobre la aritmética modular para crear algoritmos de cifra y descifrado. La teoría de la complejidad de los algoritmos estudia los problemas y los clasifica según sean tratables o intratables y se ocupa de la calidad de los algoritmos criptográficos.

Los algoritmos criptográficos tienden a degradarse en el tiempo. A medida que pasa el tiempo los algoritmos de encripción se van haciendo más fáciles de quebrar debido al avance en la velocidad y potencia de los equipos de computación. Todos los algoritmos criptográficos son vulnerables a los ataques de fuerza bruta -tratar sistemáticamente con cada posible clave de encripción, buscando colisiones para funciones hash, factorizando grandes números, etc.- la fuerza bruta se hace más fácil a medida que pasa el tiempo. Además de la fuerza bruta están los avances en las matemáticas fundamentales que permiten nuevos métodos y técnicas de criptoanálisis. La degradación de los algoritmos a través del tiempo se refleja aún más en los Algoritmos asimétricos, que en los simétricos, con el consecuente aumento de la longitud de la clave de igual forma, para mantener un nivel de seguridad constante. Debido a esto hoy en la actualidad, se recomienda, para sistemas asimétricos una longitud de la clave no inferior a 1024 bits recomendable 1200 bits y, para sistemas simétricos una longitud de clave no inferior a 80 bits.

Debido a la longitud de clave utilizada por los algoritmos asimétricos, se comportan considerablemente más lentos que los algoritmos simétricos, con lo que en la práctica, los métodos asimétricos se emplean generalmente para codificar la *clave de sesión* (simétrica), de cada mensaje o transacción particular. Además los sistemas asimétricos requieren de mucho menos administración de clave, lo cual se hace pesado y oneroso en los sistemas simétricos. Ambos sistemas se basan en la confianza para mantener en secreto ya sea la clave de un sistema simétrico o la clave privada de un sistema asimétrico, ya que la divulgación u obtención de ésta compromete a sistema, para aquellos mensajes en que se vea involucrada dicha clave.

Todo lo que se refiere al manejo de claves es algo muy complejo, ya que se debe administrar a las mismas durante todo su tiempo de vida, involucra mucho trabajo, el cual a veces se desprecia. Una forma de administrar claves públicas es a través de certificados digitales, los cuales son otorgados por autoridades

certificadoras, su estructura depende de muchos factores, pueden tener estructura jerárquica, centralizada, etc.

En la práctica se emplea una combinación de los dos sistemas, para obtener las ventajas de cada uno y minimizar las desventajas.

Más de Criptografía, en pocas palabras.... ver Transparencias

Algunas definiciones...

Criptografía: es el conjunto de técnicas (entre algoritmos y métodos matemáticos), que resuelven los problemas de autenticidad, privacidad, integridad y no rechazo en la transmisión de la información.

Texto cifrado: es el mensaje luego de ser cifrado.

Texto claro /plano: es el documento /mensaje antes de ser cifrado.

Cifrar /encriptar: es la acción que produce un texto cifrado (ilegible) a partir de un texto plano.

Descifrar /desencriptar: es la acción inversa a cifrar, convierte un texto cifrado a otro legible (texto plano).

Criptografía Simétrica: es el conjunto de métodos que permite establecer comunicación cifrada, con la característica que ambos lados de la comunicación (remitente /receptor), tienen la misma clave y6 ésta es secreta.

Criptografía Asimétrica: es el conjunto de métodos que permite establecer comunicación cifrada, donde una de las clave es pública y otra es privada (secreta). Cada usuario tiene un par de claves una pública y otra privada.

Longitud de la clave: es el número de bits (ceros y unos), que tienen las claves, y es sólo uno de los parámetros de los que depende la seguridad de un sistema criptográfico.

Certificado Digital: físicamente es un archivo de hasta 2K de tamaño que contiene principalmente, los datos de una entidad, una persona o servidor, la clave pública de esa entidad y la firma de la autoridad certificadora que es reconocida con la capacidad de poder comprobar la identidad de la persona y valida la clave pública que es asociada a la entidad.

Autoridad Certificadora: es una entidad que es reconocida para poder certificar la asociación de una clave pública a una persona o servidor.

Criptosistema: es un sistema que permite cifrar y descifrar la información y consta de cinco elementos:

- un espacio de mensajes sin cifrar **M** (lo que se denomina texto plano)
- un espacio de mensajes cifrados **C** (lo que se denomina texto cifrado o criptogramas)
- un espacio de claves **K** (conjunto de claves que pueden ser usadas en el criptosistema)
- un conjunto de transformaciones de cifrado o familia de funciones **E** que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente E_k para cada valor posible de la clave K.
- Un conjunto de transformaciones de descifrado **D**.(análogo a E)

Todo criptosistema ha de cumplir la siguiente condición: $D_k(E_k(m))=m$

Criptoanálisis: es el conjunto de métodos y técnicas usadas para comprometer la seguridad de un criptosistema. Con lo que se obtiene el texto plano y /o la clave a partir del texto cifrado sin la aplicación del algoritmo, que se supone conocido. Su objetivo es ver la información que se transmite.

Firma Digital: es una de las principales aplicaciones de la criptografía. Consiste en un mecanismo que permite verificar el origen de un mensaje y la identidad del remitente para resolver problemas de autenticidad entre el remitente y el receptor del mensaje.

Bibliografía

- **Criptografía Para Principiantes**
  (Versión 1.0)
  José de Jesús Angel Angel
  jesus@seguridata.com
- **Political Issues in the Use of Cryptography**
  December 4th, 1998
  Petri Puhakainen
  Department of Computer Science and Engineering
  Helsinki University of Technology
  Petri.Puhakainen@fi.oracle.com
- **TECNICAS Y ALGORITMOS DE ENCRIPTACION DE DATOS**
  Marco Antonio Alvarado Juárez. Bajado de Internet.
- **Documento sobre la longitud de las claves y seguridad**, Bajado de Internet. http://www.counterpane.com/keylength.html
- **La seguridad de los protocolos criptográficos**
  Taller de Criptografía - Informe 2
- **Servidores de Claves y Certificados**
  Bajado de Internet.
- **Sobre el tamaño de clave I: planteamiento.**
  Taller de Criptografía - Informe 22
- **Sobre el tamaño de clave II: predicciones.**
  Taller de Criptografía - Informe 23
- **Algo sobre Criptografía**
  Tomás Bradanovic
- **Las claves criptográficas**
  Por Oscar Cánovas Reverte
- **Criptografía y seguridad en computadoras**
  Tercera Edición (versión 1.00). Junio 2001.
  Los capítulos correspondientes a criptografía básica.

Además he leído más bibliografía tanto la mandada por la cátedra como la encontrada en Internet, pero no aportaba mayores conceptos, ni diferentes a los ya encontrados o se iva demasiado particular en el tratamiento matemático, el cual no me pareció adecuado, para el alcance de éste informe y de la materia en sí.

OBSERVACIÓN: el informe realizado, está hecho en base a los niveles de lo dado en clase y explayado en temas que me parecieron relevantes, pues debido a la gran gama de información encontrada y diferentes enfoques, se me hizo imposible poder plasmar todo, pues detallar o nombrar algunos otros temas significaba extenderme con lo que llevaría a escribir muchas hojas más, lo cual no correspondería a los topes dados en clase, que por cierto me he pasado un poco, pero poner menos significaba colocar simplemente lo de clase, lo cual no me pareció adecuado.