UNIVERSIDAD AMERICANA

Redes de comunicación

Criptografía : sistemas simétricos

Recopilación de teoría referente a la materia

Ing. Luis Müller

01/01/2011

Esta es una recopilación de la teoría referente a la asignatura Redes de Comunicación, a ser estudiada en clases con los alumnos, y que servirá como base para su aplicación también en clases en ejercicios prácticos.

Contenido

Criptografía 3
Sistemas de substitución poli alfabética 4
Criptografía simétrica 6
Funciones de Flujo 11
Funciones Hash 11
Ejemplos 14
Inconvenientes 15
Alternativas 15

Unidad II – criptografía: sistemas simétricos

Principios básicos. Características. Tipos de algoritmos. Claves simétricas. Ataques.

Criptografía

Entendemos por Criptografía (Kriptos=ocultar, Graphos=escritura) la técnica de transformar un mensaje inteligible, denominado **texto en claro**, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos **criptograma** o texto cifrado. El método o sistema empleado para encriptar el texto en claro se denomina **algoritmo de encriptación**.

La Criptografía es una rama de las Matemáticas, que se complementa con el Criptoanálisis, que es la técnica de descifrar textos cifrados sin tener autorización para ellos, es decir, realizar una especie de Criptografía inversa. Ambas técnicas forman la ciencia llamada Criptología.

La Criptografía es un arte antigua que surge, prácticamente, como un escrito. Su utilización siempre tiene connotado militar, más allá de la Segunda Guerra Mundial, como o adviento de dos computadoras, la aplicación de criptografía comprende a la "sociedad de la información".

La evolución de técnicas criptográficas permite, que el hombre haga más seguro las transacciones electrónicas, siendo la solución más indicada, hacer los problemas de garantizar la privacidad y protección de información, inclusive a través de autenticación de mensajes de la asignatura digital.

El estudio de Criptografía comienza por el método de sustitución simple que Julio César usaba para enviar mensajes a sus generales. Este método o alfabeto es dislocado de número en relación a posiciones de la clave. Asimismo, para un mensaje ser "linda" Un sistema de César cuya clave sea, por ejemplo, 3 (tres), basta hacer la siguiente substitución:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

Que sea, una palabra simple como **"atacar ahora"** seria codificada como **"xqxzxo xdlox"**. Este sistema y otros de permutación, en que las letras son "embarulladas", llegan a ser que los infantes más por mucho tiempo entendieran perfectamente un objetivo de "esconder" un mensaje.

Sistemas de substitución poli alfabética

Los sistemas de substitución simple y de permutación son muy fáciles de ser quebrados.

La tentativa de colocar más dificultades en el proceso tentativa - intención de sistema como este poli alfabético. Este sistema, no son reemplazados de un único alfabeto de substitución, son utilizados varios alfabetos permutados, trocados periódicamente con una señal de mensaje. Un objetivo principal de que van intentar desvendar el código de la clave, descubrir el período de la clave y después, los códigos usados.

Por ejemplo, una clave poli alfabética de período tres va a modificar las posiciones cero, tres, seis, etc. de mensajes de acuerdo con el primer código, las posiciones en, cuatro, siete, etc., con un segundo código y las posiciones dos, cinco, ocho, etc. con un tercero. Tómese una clave K= {3, 17,8}, tenemos:

K-1 (sistema de César 3):

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

K-2 (sistema de César 17):

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

J K L M N O P Q R S T U V W X Y Z A B C D E F G H I

K-3 (sistema de César 8):

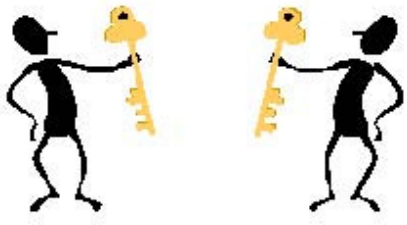
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

S T U V W X Y Z A B C D E F G H I J K L M N O P Q R

En un mensaje que tenga un texto: **"invadir a media noche"** será codificado como: **"fwnxmao j ebrs kxaqn"**

Criptografía simétrica

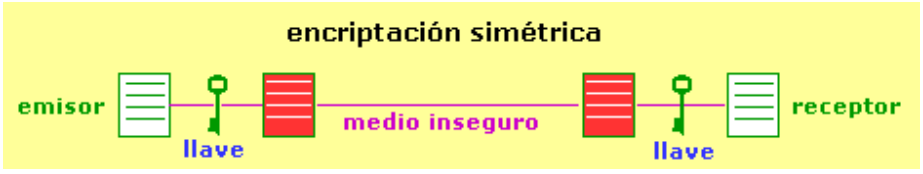
La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.



La **criptografía simétrica** es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

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

Incluye los sistemas clásicos, y se caracteriza porque en ellos *se usa la misma clave* para encriptar y para desencriptar, motivo por el que se denomina simétrica.



Toda la seguridad de este sistema está basada en la llave simétrica, por lo que es misión fundamental tanto del emisor como del receptor conocer esta clave y mantenerla en secreto. Si la llave cae en manos de terceros, el sistema deja de ser seguro, por lo que habría que desechar dicha llave y generar una nueva.

La información original que debe protegerse se denomina **texto plano** o **texto en claro**. El cifrado es el proceso de convertir el texto plano en un texto imposible de leer llamado **texto cifrado**. Para obtener un texto cifrado, se aplica un algoritmo de cifrado, utilizando una clave, al texto plano.

Cifrado de datos

De la misma manera, si aplicamos un algoritmo de descifrado, que también utiliza una clave, al texto cifrado, obtendremos, de nuevo, el texto plano.

Descifrado de datos

Un buen sistema de **cifrado** pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, *no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando*. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Los algoritmos de cifrado ampliamente utilizados tienen estas propiedades (por ejemplo: GnuPGen sistemas GNU).

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**.

DES es un sistema criptográfico, que toma como entrada un bloque de 64 bits del mensaje y este se somete a 16 interacciones, una clave de 56 bits, en la práctica el bloque de la clave tiene 64 bits, ya que a cada conjunto de 7 bits se le agrega un bit que puede ser usada como de paridad.

En las siguientes imágenes se puede observar el funcionamiento del intercambio de claves y de cifrado simétrico.

El emisor envía al receptor la clave con la cifrar y descifrar los mensajes a través de un canal seguro.

Criptografía simétrica. Intercambio de claves.

El emisor envía el mensaje cifrado al receptor. Éste último descifra el mensaje para ver su contenido.

Criptografía simétrica. Cifrado/Descifrado.

Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio. Richard Feynman fue famoso en Los Álamos por su habilidad para abrir cajas de seguridad; para alimentar la leyenda que había en torno a él, llevaba encima un juego de herramientas que incluían un estetoscopio. En realidad, utilizaba una gran variedad de trucos para reducir a un pequeño número la cantidad de combinaciones que debía probar, y a partir de ahí simplemente probaba hasta que adivinaba la combinación correcta. En otras palabras, reducía el tamaño de posibilidades de claves.

Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves posibles (72.057.594.037.927.936 claves). Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como 3DES, Blowfish e IDEA **usan claves de 128 bits**, lo que significa que existen 2 elevado a 128 claves posibles. Esto equivale a muchísimas más claves, y aun en el caso de que todas las máquinas del planeta estuvieran cooperando, tardarían más tiempo en encontrar la clave que la edad del universo.

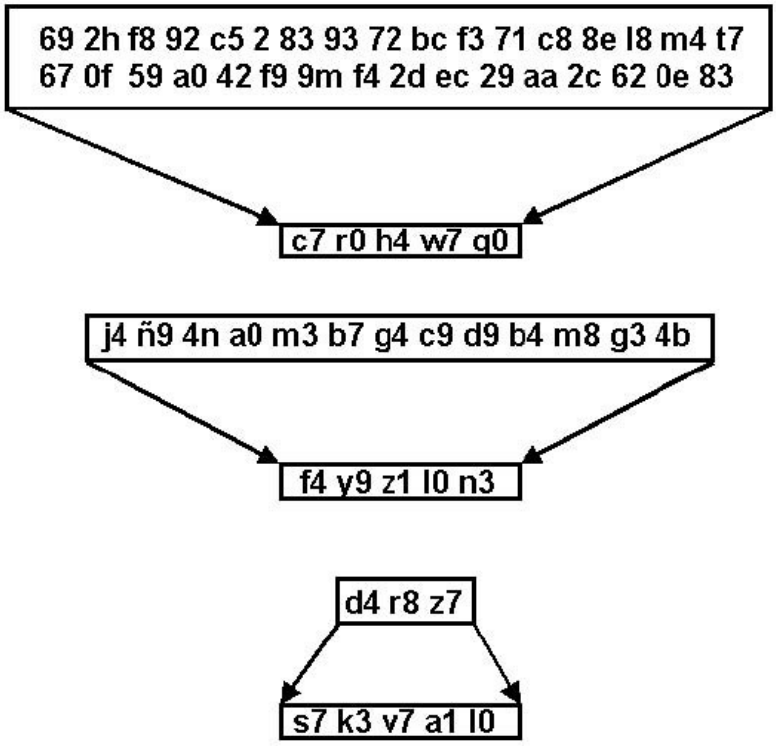
Funciones de Flujo

Los cifradores de flujo o stream ciphers, son usados donde se cuente con un ancho de banda restringido (el número de bits que se transmiten a la vez), además de que se requiere independencia en los bloques transmitidos, entonces la mejor opción es cifrar bit por bit o byte por byte, este tipo de cifradores tiene la característica además de ser muy rápido. Los algoritmos más conocidos de este tipo están **RC-4**, **SEAL** [66] y **WAKE.**

Funciones Hash

Una herramienta fundamental en la criptografía, son las funciones hash [60]. Son usadas principalmente para resolver el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen.

Una función hash es también ampliamente usada para la firma digital, ya que los documentos a firmar son en general demasiado grandes, la función hash les asocia una cadena de longitud 160 bits que los hace más manejables para el propósito de firma digital.

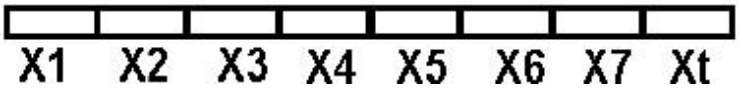


Esto es, un mensaje de longitud arbitraria lo transforma de forma “única” a un mensaje de longitud constante.

¿Cómo hace esto?

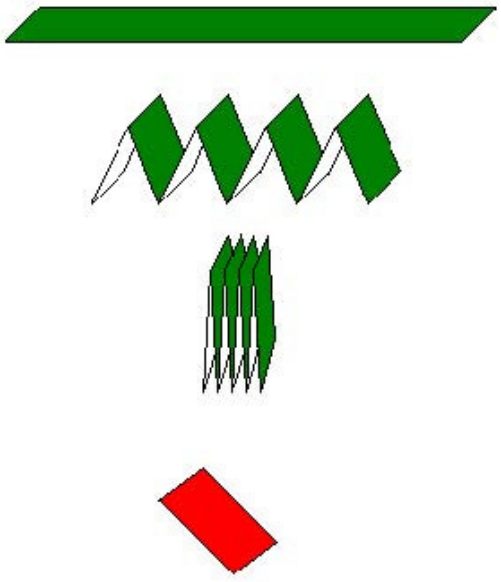
La idea general es la siguiente:

La función hash toma como entrada una cadena de longitud arbitraria, digamos 5259 bits, luego divide éste mensaje en partes iguales, digamos de 160bits; como en este caso y en general el mensaje original no será un múltiplo de 160, entonces para completar un número entero de partes de 160 bits al último se le agrega un relleno, digamos de puros ceros. En nuestro caso en 5259 caben 32 partes de 160 bits y sobran 139, entonces se agregarán 21 ceros más.



Posteriormente se asocia un valor constante a un vector inicial IV y H0=IV Ahora se obtiene H1 que es el resultado de combinar H0 con X1 usando una función de compresión *f* H1 = *f*(H0,X1) Posteriormente se obtiene H2, combinando H1 y X2 con *f* H2 = *f*(H1,X2) Se hace lo mismo para obtener H3 H3 = *f*(H2,X3) Hasta llegar a Ht Ht = *f*(Ht-1, Xt) Entonces el valor hash será *h*(M) = Ht

De alguna forma lo que se hace es tomar el mensaje partirlo en pedazos de longitud constante y combinar de alguna forma pedazo por pedazo hasta obtener un solo mensaje de longitud fija como muestra la figura siguiente:



Ejemplos

Como ejemplo de sistema simétrico está Enigma. Éste fue un sistema empleado por Alemania durante la Segunda Guerra Mundial, en el que las claves se distribuían a diario en forma de libros de códigos. Cada día, un operador de radio, receptor o transmisor, consultaba su copia del libro de códigos para encontrar la clave del día. Todo el tráfico enviado por ondas de radio durante aquel día era cifrado y descifrado usando las claves del día.

Inglaterra usó máquinas para descifrar las claves durante aquella guerra y aunque el citado sistema alemán, Enigma, estaba provisto de un amplio abanico de claves, los ingleses diseñaron máquinas de cómputo especializado, los Bombes, para comprobar las claves de modo mecánico hasta que la clave del día era encontrada. Esto significaba que algunas veces encontraban la clave del día pocas horas después de que ésta fuera puesta en uso, pero también que otros días no podían encontrar la clave correcta. Los Bombes no fueron máquinas de cómputo general, sino las precursoras de los ordenadores (computadoras) actuales.

Algunos ejemplos de algoritmos simétricos son:

DES, 3DES, RC5, AES, Blowfish e IDEA.

Inconvenientes

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

Otro problema es el número de claves que se necesitan. Si tenemos un número **n** de personas que necesitan comunicarse entre sí, se necesitan **n**/**2** claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Alternativas

Para solucionar este problema existen la criptografía asimétrica y la criptografía híbrida.

La criptografía asimétrica será estudiada en la Unidad III.