Revista Digital Universitaria
10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

ARTICULO

INTRODUCCIÓN A LA CRIPTOGRAFÍA

Gibrán Granados Paredes
Ingeniero en Computación
gibran@uxmcc2.iimas.unam.mx

http://www.revista.unam.mx/vol.7/num7/art55/int55.htm

INTRODUCCIÓN A LA CRIPTOGRAFÍA

Resumen

La criptografía es una herramienta muy útil cuando se desea tener seguridad informática; puede ser también entendida como un medio para garantizar las propiedades de confidencialidad, integridad y disponibilidad de los recursos de un sistema.

Con la criptografía se puede garantizar las propiedades de integridad y confidencialidad, pero hay que saber cómo utilizarla, para ello es importante tener claros los conceptos básicos que están detrás de los sistemas criptográficos modernos. Estos conceptos van desde entender qué es la criptografía, cómo está clasificada, entender el funcionamiento básico de algunos sistemas de cifrado y conocer cómo se forman los documentos digitales como firmas y sobres digitales.

Palabras clave: Criptografía, cifrado, seguridad informática, firmas digitales, sobres digitales.

INTRODUCTION TO THE CRIPTOGRAPHY

Abstract

The cryptography is a useful tool to keep the information security. The information security tries to keep the integrity, confidentiality and availability of the system resources.

The attributes of integrity and confidentiality can be guaranteed by cryptography, to do that we have to know how to use it and keep in mind the concepts of the modern cryptography. The concepts are: the cryptography definition and classification, how the cryptosystems works and how the digital documents are made, like digital signatures and digital envelopes.

Keywords: Cryptography, cipher, information security, digital signatures, digital envelopes.

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

Seguridad y Criptografía

La necesidad de Seguridad de la Información en una organización ha cambiado en las últimas décadas. Antes del uso de las computadoras, la Seguridad de la Información era proporcionada por medios físicos, por ejemplo el uso de cajas fuertes y por medidas administrativas, como los procedimientos de clasificación de documentos.

Con el uso de la computadora, y más aún con la llegada de Internet, fue indispensable el uso de herramientas automatizadas para la protección de archivos y otro tipo de información almacenada en la computadora, algunas de estas herramientas son los cortafuegos, los Sistemas Detectores de Intrusos y el uso de sistemas criptográficos. Estas herramientas no sólo permiten proteger a la información, sino también a los Sistemas Informáticos que son los encargados de administrar la información.

De la necesidad por proteger a la información y a los sistemas que la administran surge el término de Seguridad Informática.

En este punto hay que hacer una breve pausa para aclarar el hecho de que actualmente los términos de seguridad, seguridad de la información y de seguridad informática han sido empleados de diversas maneras y se les han dado diversos significados de acuerdo al contexto. Los siguientes párrafos son definiciones que tratan de ilustrar uno de los significados más comunes a cada término.

a) Seguridad:

De acuerdo con el diccionario de la Real Academia Española, seguridad es:

- Cualidad de seguro.
- Dicho de un mecanismo: Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente.

b) Seguridad de la Información:

Se puede hablar de la Seguridad de la Información como el conjunto de reglas, planes y acciones que permiten asegurar la información manteniendo las propiedades de confidencialidad, integridad y disponibilidad de la misma.

- La *confidencialidad* es que la información sea accesible sólo para aquéllos que están autorizados.
- La *integridad* es que la información sólo puede ser creada y modificada por quien esté autorizado a hacerlo.
- La *disponibilidad* es que la información debe ser accesible para su consulta o modificación cuando se requiera.

c) Seguridad Informática:

Conjunto de políticas y mecanismos que nos permiten garantizar la confidencialidad, la integridad y la disponibilidad de los recursos de un sistema (entiéndase recursos de un sistema como memoria de procesamiento, espacio de almacenamiento en algún medio físico, tiempo de procesamiento, ancho de banda y por su puesto la información contenida en el sistema).

De acuerdo con las definiciones anteriores para que exista seguridad ya sea de la información o informática hay que garantizar las propiedades de confidencialidad, integridad y disponibilidad. Y es aquí donde se utiliza a la criptografía, ya que mediante el uso correcto de sistemas criptográficos se pretende garantizar las propiedades de confidencialidad e integridad. Veamos el siguiente ejemplo que ilustra una comunicación.

Primeramente se muestra lo que idealmente es una comunicación normal, en este caso no existe ningún problema de seguridad informática. El mensaje que se envía se recibe sin alteración alguna.

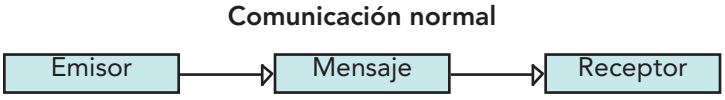

Figura 1. Comunicación normal

El segundo caso muestra uno de los problemas más grandes que hay, la interrupción de la transmisión del mensaje, que puede ser ocasionada por fallo del canal o de algún elemento del sistema de comunicación, ya sea de forma natural o intencional. Esto es traducido a un problema de *disponibilidad*.

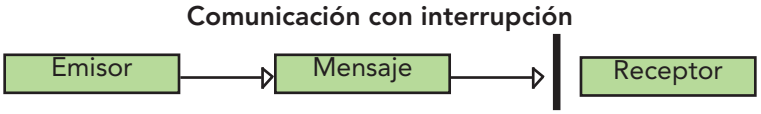

Figura 2. Comunicación con Interrupción

La interceptación de los datos por un intruso (un intruso es un ente externo al sistema) es algo muy común dentro de las comunicaciones, ya que muchas de las transmisiones son enviadas mediante protocolos que son conocidos por todos y a los mensajes no se les hace ningún tratamiento especial, en otras palabras, viajan tal cual se generan. Lo único que se hace es escuchar todo lo que pasa por el canal sin alterar nada. Este es un problema de *confidencialidad*.

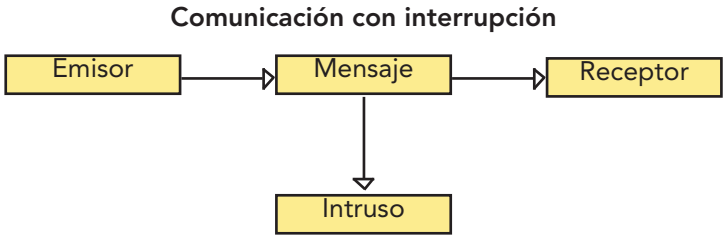

Figura 2. Comunicación con interceptación

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

Otro problema en la comunicación es el problema de la falsificación. Esto se produce cuando el intruso captura un mensaje, se adueña de él y de la identidad del emisor y genera un nuevo mensaje con la identidad del emisor. Este es un problema de *integridad* y *confidencialidad*.

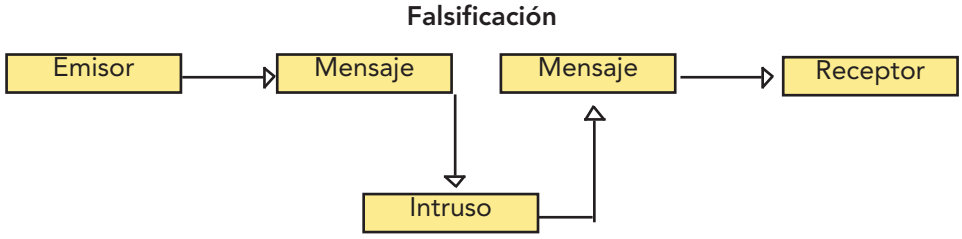

Figura 4. Comunicación con Falsificación

Finalmente la generación de mensajes se da cuando el intruso genera un mensaje engañando al receptor haciéndolo creer que es un emisor válido. Esto se traduce en un problema de *integridad*.

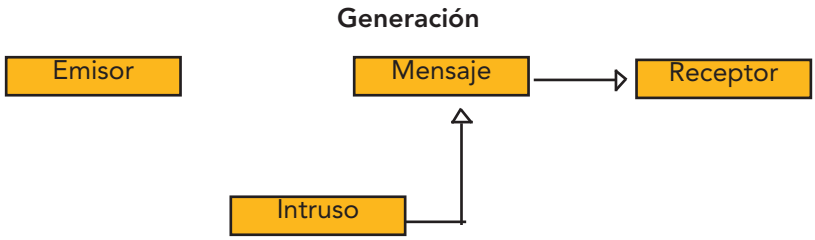

Figura 5. Generación de una comunicación apócrifa

Es muy fácil ver como una comunicación y un sistema informático son muy similares, ya que en un sistema informático se procesan, almacenan, envían y reciben datos.

Ahora, si pudiéramos de alguna forma evitar los problemas de disponibilidad, integridad y confidencialidad, tendríamos un sistema "seguro". Para lograr esto tendríamos que aislar al sistema de los intrusos y hacerlo anti-fallos lo cual es prácticamente imposible. Lo que se hace es crear mecanismos que garanticen en cierta medida las propiedades de disponibilidad, integridad y confidencialidad.

La disponibilidad, generalmente, se trata de solucionar con sistemas redundantes.

La confidencialidad se puede lograr usando un mecanismo que, aunque sea robada la información, permita que no se pueda acceder a ésta o garantice de alguna forma que no se pueda llegar a ella, hasta que pierda su valor.

La integridad es más difícil de lograr y se hace con el uso de varios mecanismos que garantizan la identidad de un ente que está autorizado por el sistema para crear o hacer modificaciones a la información, de tal forma que se puede verificar posteriormente quién creó o modificó la información. Además estos mecanismos permiten ver si la información ya creada ha sufrido o no alguna modificación no autorizada.

Los mecanismos para garantizar la integridad y la confidencialidad se implementan con sistemas criptográficos, de ahí la importancia de la criptografía en la seguridad informática en los sistemas actuales.

Criptografía

La palabra criptografía proviene en un sentido etimológico del griego *Kriptos=ocultar, Graphos=escritura,* lo que significaría ocultar la escritura, o en un sentido más amplio sería aplicar alguna técnica para hacer ininteligible un mensaje.

En su clasificación dentro de las ciencias, la criptografía proviene de una rama de las matemáticas, que fue iniciada por el matemático Claude Elwood Shannon en 1948, denominada: "Teoría de la Información". Esta rama de las ciencias se divide en: "Teoría de Códigos" y en "Criptología". Y a su vez la Criptología se divide en Criptoanálisis y Criptografía, como se muestra en la siguiente figura:

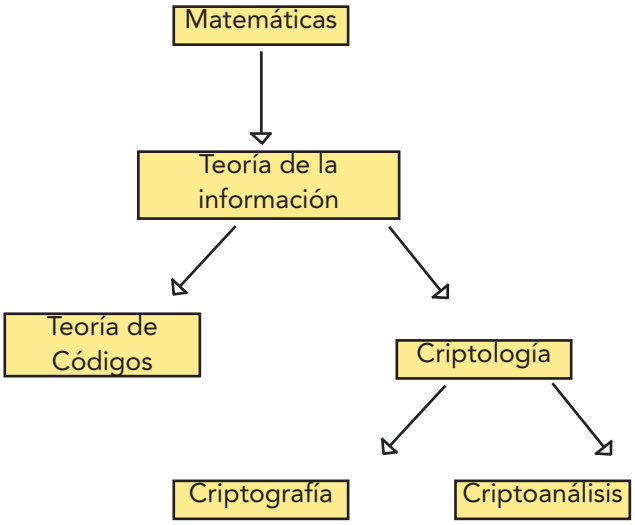

Figura 6. Origen de la Criptografía

En un sentido más amplio, la Criptografía es la ciencia encargada de diseñar funciones o dispositivos, capaces de transformar mensajes legibles o en claro a mensajes cifrados de tal manera que esta transformación (cifrar) y su transformación inversa (descifrar) sólo pueden ser factibles con el conocimiento de una o más llaves.

En contraparte, el criptoanálisis es la ciencia que estudia los métodos que se utilizan para, a partir de uno o varios mensajes cifrados, recuperar los mensajes en claro en ausencia de la(s) llave(s) y/o encontrar la llave o llaves con las que fueron cifrados dichos mensajes.

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

Clasificación de la criptografía

La criptografía se puede clasificar históricamente en dos: La criptografía clásica y la criptografía moderna.

La criptografía clásica es aquella que se utilizó desde antes de la época actual hasta la mitad del siglo XX. También puede entenderse como la criptografía no computarizada o mejor dicho no digitalizada. Los métodos utilizados eran variados, algunos muy simples y otros muy complicados de criptoanalizar para su época.

Se puede decir que la criptografía moderna se inició después de tres hechos: el primero fue la publicación de la "Teoría de la Información" por Shannon; el segundo, la aparición del estándar del sistema de cifrado DES (Data Encryption Standard) en 1974 y finalmente con la aparición del estudio realizado por Whitfield Diffie y Martin Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifrado, denominado cifrado de llave pública en 1976.

Tanto la criptografía clásica como la moderna se clasifican de acuerdo a las técnicas o métodos que se utilizan para cifrar los mensajes. Esta clasificación la podemos ver en la siguiente figura:

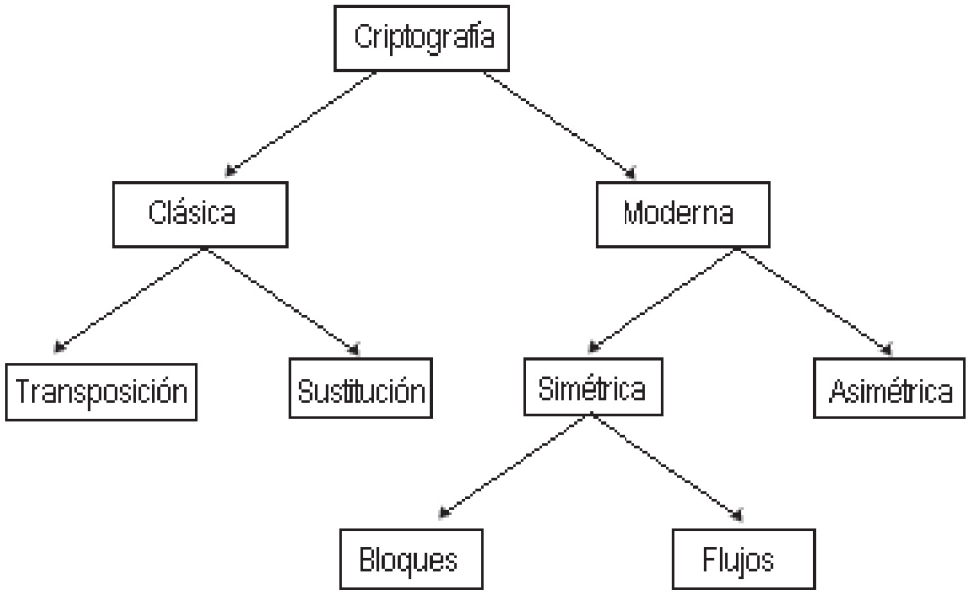

Figura 7. Clasificación de la Criptografía

Criptografía Clásica

Como ya se mencionó anteriormente, la criptografía clásica es muy antigua. Las técnicas criptográficas eran muy ingeniosas y se usaban para enviar mensajes secretos entre las personas que tenían el poder o en época de guerra para enviar instrucciones. A diferencia de la criptografía moderna, el algoritmo del sistema criptográfico se mantenía en secreto. La criptografía clásica también incluye la construcción de máquinas, que mediante mecanismos, comúnmente engranes o rotores, transformaban un mensaje en claro a un mensaje cifrado, como la máquina Enigma usada en la Segunda Guerra Mundial.

La siguiente figura ilustra la clasificación de la criptografía clásica:

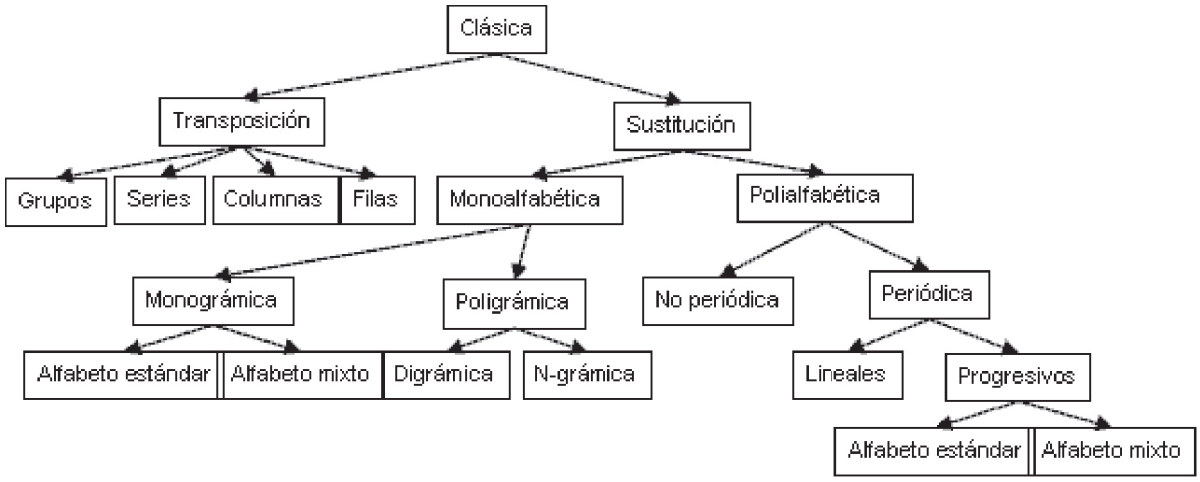

Figura 8. Clasificación de la Criptografía Clásica

Los cifradores por *transposición* utilizan la técnica de permutación de forma que los caracteres del texto se reordenan mediante un algoritmo específico.

Los cifradores por *sustitución* utilizan la técnica de modificación de cada carácter del texto en claro por otro correspondiente al alfabeto de cifrado. Si el alfabeto de cifrado es el mismo que el del mensaje o bien el único, hablamos entonces de cifradores *monoalfabéticos*; es decir, existe un único alfabeto en la operación de transformación del mensaje en criptograma. Por el contrario, si en dicha operación intervienen más de un alfabeto, se dice que el cifrador es *polialfabético*.

Es realmente interesante analizar cada una de las técnicas anteriores, en este documento sólo se verán dos técnicas: un cifrado de transposición de grupos, la escítala, y un ejemplo de sustitución monoalfabética, monográmica con el alfabeto estándar, el cifrado César.

La escítala

En siglo V a.c. los lacedemonios, un antiguo pueblo griego, usaban el método de la *escítala* para cifrar sus mensajes. El sistema consistía en una cinta que se enrollaba en un bastón sobre el cual se escribía el mensaje en forma longitudinal, como se muestra en la siguiente figura:

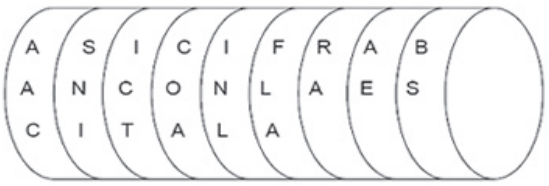

Figura 9. Escítala

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

Una vez escrito el mensaje, la cinta se desenrollaba y era entregada al mensajero. Para enmascarar completamente la escritura es obvio que la cinta en cuestión debe tener caracteres en todo su contorno. Como es de esperar, la llave del sistema residía precisamente en el diámetro de aquel bastón, de forma que solamente el receptor autorizado tenía una copia exacta del mismo bastón en el que enrollaba el mensaje recibido y, por tanto, podía leer el texto en claro.

El cifrado César

En el siglo I a.c. aparece un método de cifrado conocido con el nombre genérico de cifrado de César en honor al emperador Julio César y en el que ya se aplica una transformación al texto en claro de tipo monoalfabética. El cifrado del César aplica un desplazamiento constante de tres caracteres al texto en claro, de forma que el alfabeto de cifrado es el mismo que el alfabeto del texto en claro, pero desplazado 3 espacios hacia la derecha módulo n, con n el número de letras del mismo. A continuación se muestra el alfabeto y la transformación que realiza este cifrador por sustitución de caracteres para el alfabeto castellano de 27 letras.

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

Así con este alfabeto podemos cifrar el siguiente mensaje:
Mensaje original: MENSAJE DE PRUEBA
Mensaje cifrado: OHPVDM GH SUXHED

Al describir el cifrado de César se utilizó un concepto muy usado en las matemáticas y más en criptografía: el módulo.
El módulo es una operación binaria que se realiza en los enteros positivos y se representa de la siguiente forma: $c = a \bmod b$ de tal forma que a, b y c son enteros positivos.
El valor de c al realizar la operación $c = a$ modulo b es igual al residuo de dividir a entre b. Se puede observar claramente que $0 <= c < b$.

Con este antecedente podemos escribir en forma matemática el cifrado de César de la siguiente forma:
Para cifrar

$Ci = (3 + Mi) \bmod 27$
con i= 0,1,…,n ; n = número de letras del mensaje
donde Ci es la letra cifrada y Mi es la letra a cifrar
el alfabeto comienza con A = 0 , B=1, …, Z=26

Para descifrar

$Mi = (Ci - 3) \bmod 27 = (Ci + 24) \bmod 27$
con i= 0,1,…,n ; n = número de letras del mensaje
donde Ci es la letra cifrada y Mi es la letra a cifrar
el alfabeto comienza con A = 0 , B=1, …, Z=26

Criptografía Moderna

La criptografía moderna se puede clasificar en dos grandes grupos: la criptografía de llave secreta o asimétrica y la criptografía de llave pública o asimétrica.

Criptografía Simétrica

La criptografía simétrica o de llave secreta es aquella que utiliza algún método matemático llamado sistema de cifrado para cifrar y descifrar un mensaje utilizando únicamente una llave secreta. Se puede observar en la siguiente figura que la línea punteada es el eje de simetría: lo mismo que hay de un lado existe exactamente igual en el otro, esto ilustra el hecho del porqué se le da el nombre de criptografía simétrica.

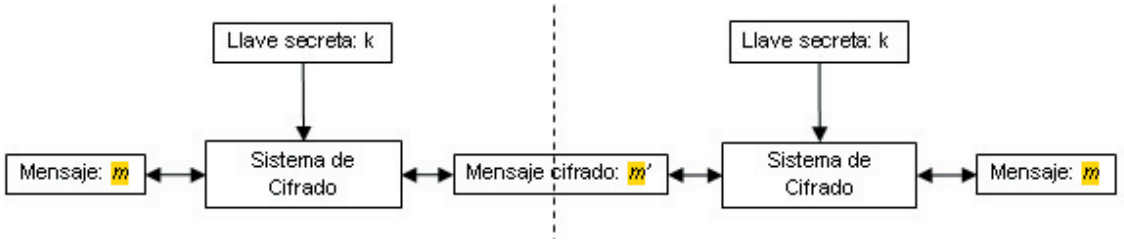

Figura 10. Criptografía simétrica

Este tipo de criptografía sólo utiliza una llave para cifrar y descifrar, esto es: si yo cifro un mensaje *m* con una llave secreta *k* entonces el mensaje cifrado resultante *m'* únicamente lo voy a poder descifrar con la misma llave *k*. Este tipo de llave conocida como secreta se debe de compartir entre las personas que se desea que vean los mensajes.
Con este tipo de criptografía podemos garantizar la confidencialidad porque únicamente quien posea la llave secreta será capaz de ver el mensaje.
El problema con la criptografía simétrica es que si yo quisiera compartir secretos con *m* personas, para cada persona tendría que generar una nueva llave secreta y la administración personal de todas *m* llaves sería un caos.
Otro problema asociado con este tipo de criptografía es cómo comparto con otra persona de una forma confidencial e integra la llave secreta.
Estos problemas se resuelven de cierta manera con criptografía asimétrica.

Criptografía Simétrica por Bloques

Este tipo de criptografía esta basado en el diseño propuesto por Horst Feistel en los años 70.

Diseño de Feistel

Un bloque de tamaño N bits comúnmente N=64 ó 128 bits se divide en dos bloques de tamaño N/2, A y B. A partir de aquí comienza el proceso de cifrado y consiste en aplicar una función unidireccional (muy difícil de invertir) a un bloque B y a una subllave k1 generada a partir de la llave secreta. Se mezclan el bloque A con el resultado de la función mediante un XOR. Se permutan los bloques y se repite el proceso n veces. Finalmente se unen los dos bloques en el bloque original. Como se ilustra en la siguiente figura:

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

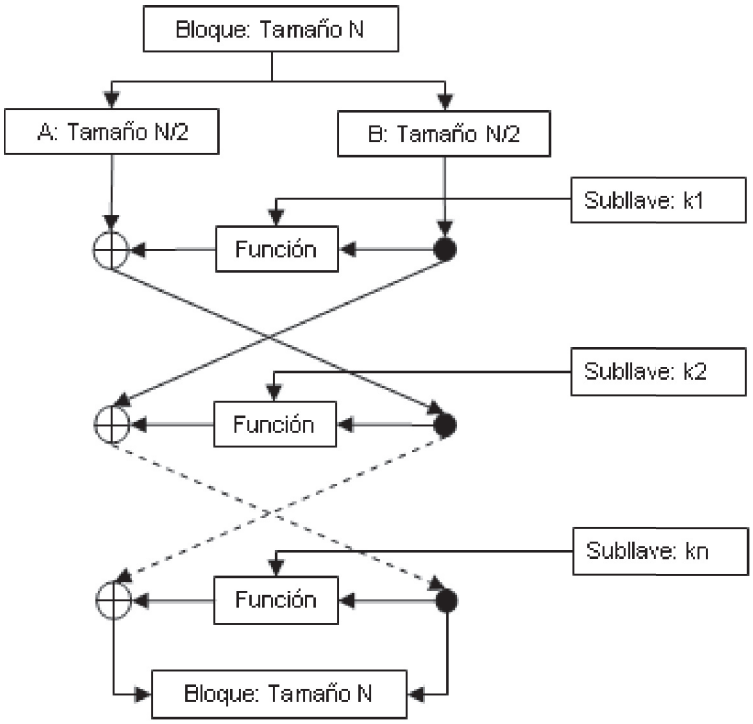

Figura 11. Cifrado por bloques de Feistel

Algunos de los sistemas criptográficos que utilizan esta filosofía son:

Tabla 1. Algoritmos de cifrado de bloque

Algoritmo	Bloque (bits)	Llave (bits)	Vueltas
Lucifer	128	128	16
DES	64	56	16
Loki	64	64	16
CAST	64	64	8
Blowfish	64	Variable	16

A lo largo de la historia de la criptografía moderna se han usado diversos métodos de cifrado, siendo el más usado el Estándar de Cifrado de Datos por sus siglas en ingles DES (Data Encryption Standard). El problema con este estándar es el tamaño de su llave: 56 bits, para tratar de corregir esto se propuso el triple DES que únicamente aplica 3 veces el DES, cifrando, descifrando y cifrando con llaves diferentes de tamaño 56 bits, incrementando el tamaño de la llave hasta 168 bits.

A finales de 2001 surge, a partir de un concurso, un nuevo estándar para el cifrado de datos. A este algoritmo conocido como Rijndael se le dio el nombre de Estándar Avanzado de Cifrado o AES (Advanced Encryption Standar). Este algoritmo no sigue la filosofía de Feistel, pero es un cifrador de bloques. Sus características son:

Tabla 2. Características del AES

Algoritmo	Bloque (bits)	Llave (bits)	Vueltas
Rijndael	128	128 ó más	flexible

Los cifrador por bloques, como se puede observar en las tablas anteriores, operan con bloques de tamaño fijo, a menudo de 64 o 128 bits. Para cifrar mensajes de mayor tamaño se usan diferentes modos de operación. Estos modos de cifrado son el ECB (Electronic codebook) libro de códigos electrónico, CBC (Cipher-block chaining) cifrado en bloque encadenado, OFB (Output Feedback) cifrado realimentado y CFB (Cipher Feedback) salida realimentada, aseguran la confidencialidad, pero no aseguran la integridad del mensaje.

Criptografía Simétrica de Flujo

Este tipo de criptografía se basa en hacer un cifrado bit a bit, esto se logra usando la operación XOR, representada con Å. Se utiliza un algoritmo determinístico que genera una secuencia pseudoaletoria de bits que junto con los bits del mensaje se van cifrando utilizando a operación XOR.

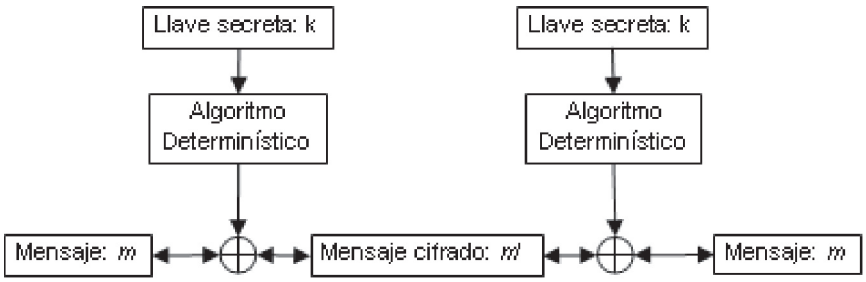

Figura 12. Criptografía simétrica de flujo

Algunos ejemplos de este tipo de criptografía son RC4 (usado en redes inalámbricas), A5 (usado en telefonía celular).

Criptografía Asimétrica

Si se observa la siguiente figura, que ilustra la idea de criptografía de llave pública, se puede ver claramente que no existe simetría en ella, ya que de un lado de la figura se cifra o descifra con una llave pública y en el otro lado con una privada. De este hecho es de donde la criptografía asimétrica debe su nombre.

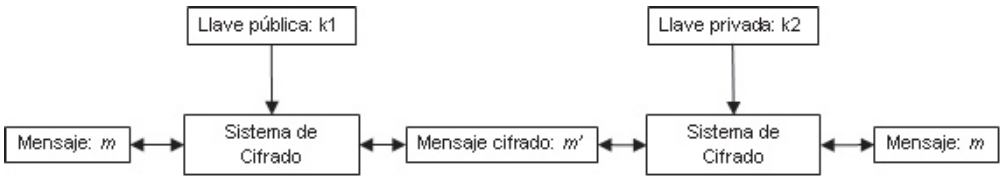

Figura 13. Criptografía asimétrica

Es importante destacar que para este tipo de criptografía lo que se cifra con una llave se puede descifrar con la otra llave. Es decir, yo puedo cifrar con la llave pública y descifrar con la privada y viceversa. Esto es de gran ayuda ya que el número de llaves que debo de poseer se reduce considerablemente. Si alguien quisiera enviar un mensaje cifrado a n personas, necesitaría saber n llaves públicas una de cada persona, pero si n personas le quiere enviar un mensaje cifrado sólo es necesario que los demás conozcan su llave

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

pública. Así, sólo tengo que preocuparme de que la llave pública sea de la persona que dice ser. Este es el problema de la criptografía asimétrica, la autenticidad de las llaves públicas.

Algunos ejemplos de este tipo de criptografía son RSA, El Gamal y Curvas Elípticas.

Solución al problema de intercambio de llaves secretas usando criptografía asimétrica: se supone que alguien va a enviar la llave secreta k a una persona para que puedan cifrar entre ellos mensajes. Lo que se hace es que se toma la llave pública de la persona a la que se le va a enviar el mensaje y se cifra con un sistema asimétrico la llave secreta, esto implica que sólo la persona poseedora de la llave privada pueda descifrar lo que se está enviando y con ello tener la llave secreta, tal y como se muestra en la siguiente figura.

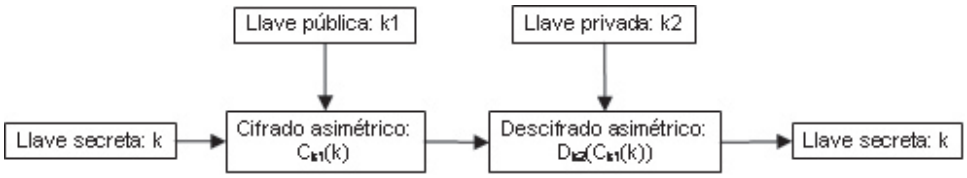

Figura 14. Intercambio de llaves secretas

Documentos digitales

En criptografía existen deferentes documentos digitales que se usan para garantizar las propiedades de confidencialidad e integridad, estos documentos son la integración de los dos tipos de criptografía: la simétrica y la asimétrica. Al hacer esta integración se compensan las desventajas de los tipos de cifrado y se utilizan las mejores características de cada uno, combinando rapidez del cifrado simétrico con la facilidad de la administración de llaves del cifrado asimétrico.

Firmas digitales

Una firma digital es un documento que permite garantizar la integridad de un documento y se puede relacionar de manera única al firmante con su firma, ya que realiza ésta con la llave privada y únicamente el firmante posee esa llave, ésto se traduce en que se verifica la autenticidad del firmante.

Antes de entrar más en detalle de cómo se realizan las firmas digitales, es importante hablar de una función denominada "Hash" o resumen del documento. Esta función lo que hace es que a partir de un documento de tamaño N bits entrega una cadena de M bits. No hay límite para el tamaño de N, pero M siempre es de tamaño constante de acuerdo con el algoritmo usado, normalmente es de 128 o 256 bits. Una de las características de este tipo de funciones es que son unidireccionales, es decir, que debe de ser imposible a partir del resumen del documento encontrar el mensaje original. También deben cumplir la propiedad de dispersión, lo que significa que si se cambia al menos un bit del documento, su resumen debe de cambiar la mitad de sus bits aproximadamente.

La firma de un documento *d* se realiza tomando un documento digital, se extrae el resumen del documento *H(d)* y este resumen se cifra asimétricamente con la llave privada del firmante *Ck1(H(d))*, esto es lo que vendría siendo la firma digital, ahora hay que ponérsela al documento, para eso se concatenan el documento y su resumen cifrado.

Ahora hay que verificar la firma, para eso se separan el documento *d* del resumen cirado. Se descifra asimétricamente con la llave pública *k2* del firmante el resumen cifrado *Dk2(Ck1(H(d)))* obteniéndose el resumen del documento original *H(d)*. Se obtiene el resumen del documento enviado *H(d)'* se comparan las dos digestiones *H(d)= H(d)'* y si estos son iguales, se dice que la firma es válida, de lo contrario es inválida. Si la firma es inválida puede deberse a dos causas: una es que se está usando una llave pública que no corresponde con la privada del firmante (problema de autenticación) o la otra es que el documento que se envió fue alterado (problema de integridad). La siguiente figura ilustra el proceso descrito de firmar y validar la firma digital.

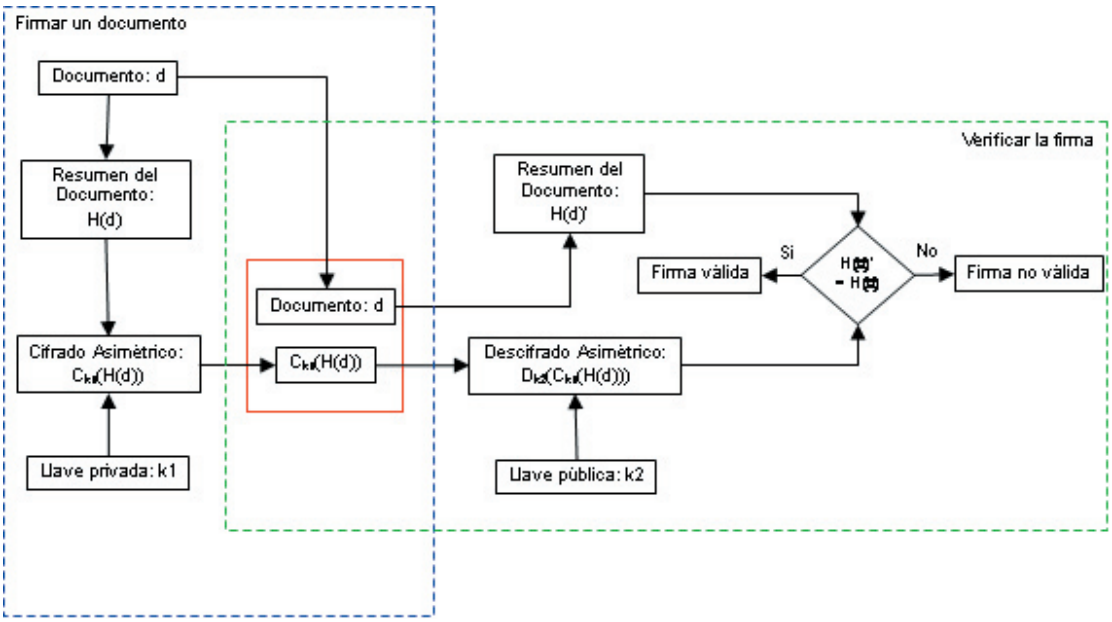

Figura 15. Firma digital

Sobres digitales

Con un sobre digital se pueden garantizar las propiedades de confidencialidad de un documento. El sobre digital usa criptografía simétrica y asimétrica. Un sobre digital se genera a partir de un documento *d* y una llave secreta *k* que se genera de forma aleatoria, se cifra simétricamente *Ck(d)* el documento d con la llave secreta k, luego la llave secreta k se cifra asimétricamente con la llave pública *k2* de la persona a la que le vamos a enviar el sobre *Ck2(k)* y finalmente se concatenan el cifrado del documento *Ck(d)* con el cifrado de la llave secreta *Ck2(k)* dando origen al sobre digital.

Para abrir el sobre digital se toma el cifrado de la llave secreta *Ck2(k)* y se descifra *Dk1(Ck2(k))* con la llave privada *k1* de la persona a la que va dirigida el sobre, obteniendo la llave secreta *k*. Con la llave *k* se descifra el cifrado del documento *Dk(Ck(d))* obteniendo así el documento d original. Esto se puede ver gráficamente en la siguiente figura.

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

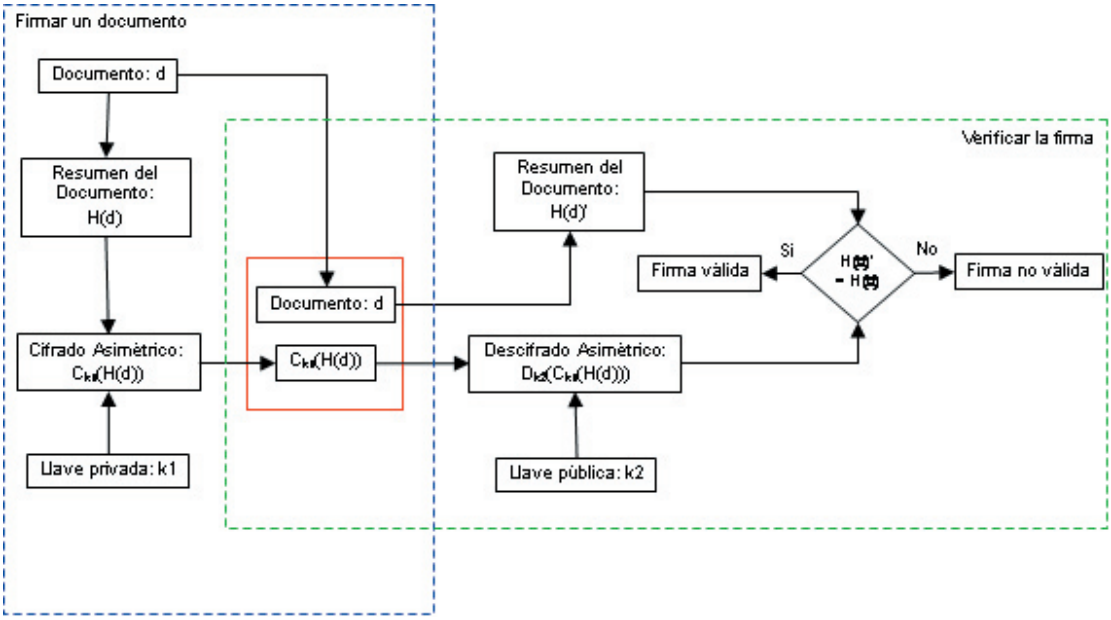

Figura 16. Sobre digital

Ahora bien, se pueden combinar los sobres digitales con las firmas digitales dando lugar a un sobre firmado y así se garantizan las propiedades de integridad, confidencialidad y autenticación.

Certificados digitales:

Un certificado digital básicamente es un documento digital expedido por una autoridad de confianza que contiene los datos que identifican al dueño del certificado, su llave pública, fecha de expedición, fecha de caducidad, los datos de la autoridad de confianza y finalmente todo esto está firmado por la misma autoridad.

Los certificados sirven para establecer lazos de confianza entre sistemas o personas, ya que si se confía en la autoridad de confianza entonces se puede confiar en la llave pública del dueño del certificado. Tratando así de resolver el problema de relacionar las identidades con las llaves públicas.

Como podemos observar, la criptografía no es la panacea, pero bien usada puede ser de gran ayuda para mantener la seguridad informática.

Conclusión

La pregunta que debe de surgirle al lector es: ¿realmente con el uso de la criptografía moderna podemos garantiza las propiedades de integridad y confidencialidad y con ello resolver casi en su totalidad el problema de la seguridad informática? La respuesta es si, por lo menos de manera teórica si.

Pero no hay que dejarnos engañar, la criptografía tiene su lado débil y en esencia son dos los factores que la debilitan: un sistema mal diseñado y el factor humano.

Del lado del sistema, como con todo sistema, hay que pasar los conceptos teóricos a un programa de cómputo y no es trivial hacer ésto, un error en una línea de código produciría lo que se le conoce como bugs del sistema debilitando o poniendo en riesgo al sistema. Ahora, si el sistema tiene los elementos más modernos de criptografía, pero está mal programado o se usan llaves demasiado pequeñas, ocurre otro riesgo muy importante que puede debilitar a la seguridad informática.

Al analizar como repercute el factor humano en un sistema se puede ver que éste siempre es el eslabón más débil en un esquema de seguridad. Ésto se debe en gran medida a la falta de capacitación en cuanto al uso de la tecnología y a que muchas veces los usuarios comparten las llaves. Otro detalle es que entre más elementos criptográficos se agreguen al sistema, es más complicado que el usuario los entienda y los use.

Por lo anterior, siempre es importante conocer un poco de criptografía, aunque sea los elementos básicos, para por lo menos tener una idea de qué tanta seguridad informática ofrece el sistema que se usa.

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

Bibliografía

RAMIO, Aguirre Jorge, *Libro Electrónico de Seguridad Informática y Criptografía*, Versión 4.1 de 1 de marzo de 2006, http://www.criptored.upm.es/guiateoria/gt_m001a.htm

STALLINGS, Wiliam, *Fundamentos de Seguridad en Redes Aplicaciones y Estándares*, Pearson, Prentice Hall, Segunda Edición 2004

FUSTER, Sabater Amparo, *Tecnicas de Criptograficas en Proteccion de Datos*, Alfaomega Grupo Editor, 2001

CABALLERO, Gil Pino, *Introduccion a la Criptografia*, Editorial Rama, 1997

Federal Information Processing Standards, Publication 81, DES Modes of operation, http://www.itl.nist.gov/fipspubs/fip81.htm

MENEZES, J. Alfred, *Handbook of Applied Cryptography*, http://www.cacr.math.uwaterloo.ca/hac/