3. Protección de Datos

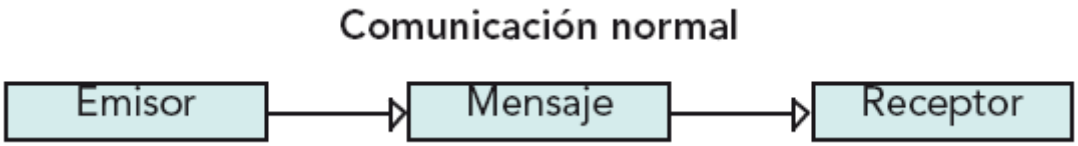
6. Criptografía

6.1 Introducción

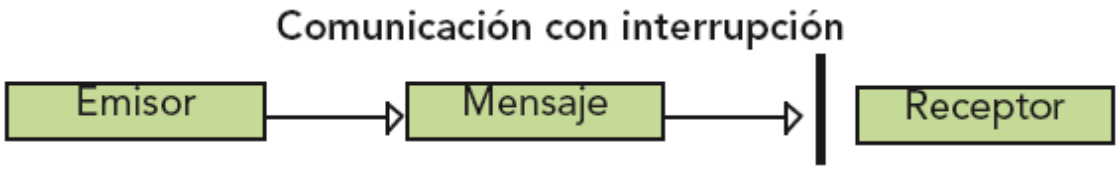
La criptografía es una herramienta muy útil cuando se desea tener seguridad informática; puede ser también entendida como un medio para garantizar las propiedades de confidencialidad, integridad y disponibilidad de los recursos de un sistema.

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.

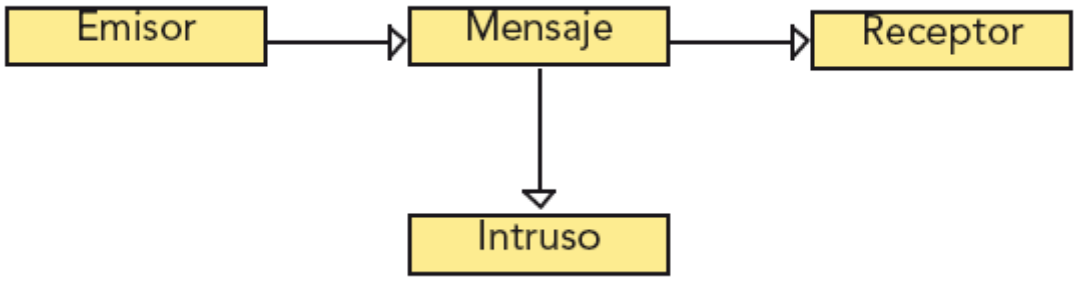


El segundo caso muestra uno de los problemas más grandes que hay, la interrupción de la transmisión del mensaje, que puede ser ocasionada por fallo del canal o de algún elemento del sistema de comunicación, ya sea de forma natural o intencional. Esto es traducido a un problema de disponibilidad.



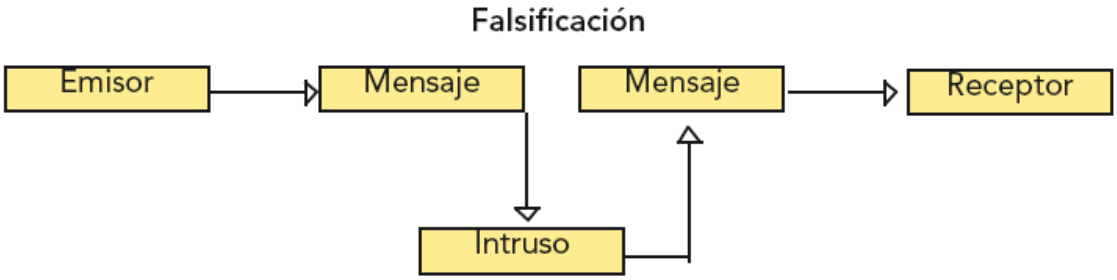
La interceptación de los datos por un intruso (un intruso es un ente externo al sistema) es algo muy común dentro de las comunicaciones, ya que muchas de las transmisiones son enviadas mediante protocolos que son conocidos por todos y a los mensajes no se les hace ningún tratamiento especial, en otras 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.

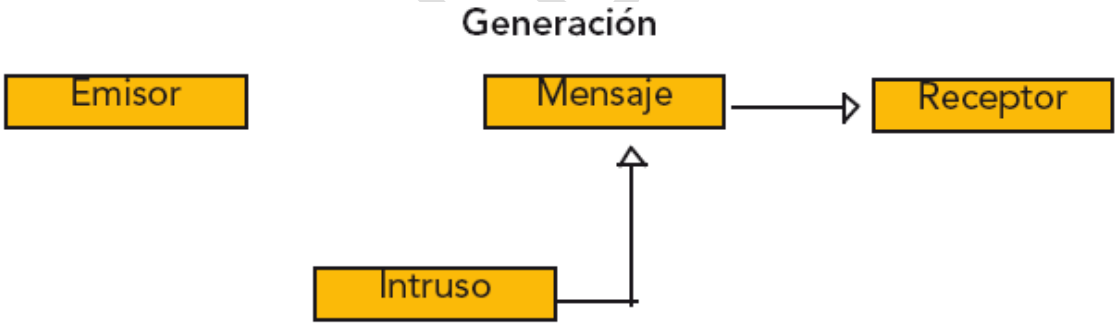


Otro problema en la comunicación es el problema de la falsificación. Esto se produce cuando el intruso captura un mensaje, se adueña de él y de la identidad del emisor y genera un nuevo mensaje con la identidad del emisor.

Este es un problema de integridad y confidencialidad.



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.



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.

6.2 Criptografía

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.

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.

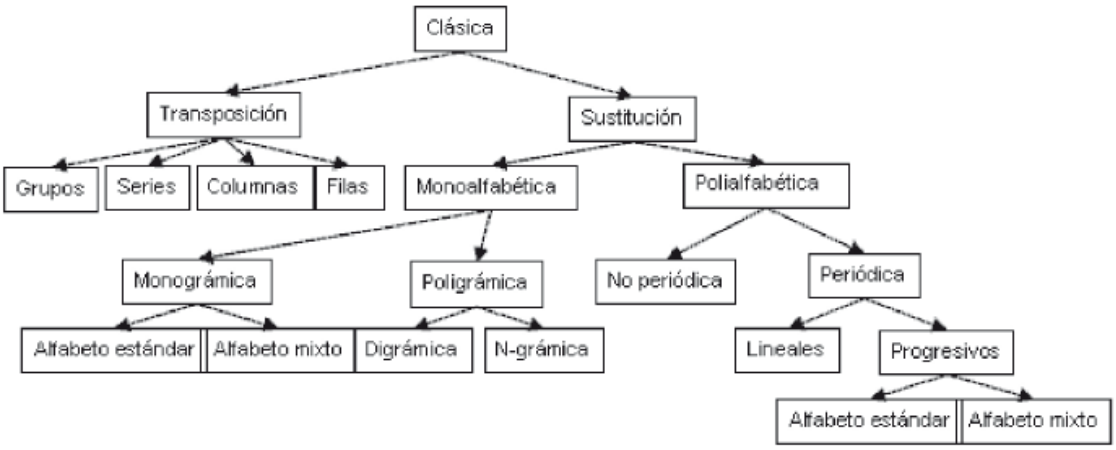
En un sentido más amplio, la Criptografía es la ciencia encargada de diseñar funciones o dispositivos, capaces de transformar mensajes legibles o en claro a mensajes cifrados de tal manera que esta transformación (cifrar) y su transformación inversa (descifrar) sólo pueden ser factibles con el conocimiento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

6.2.1 Criptografía Clásica

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.

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.



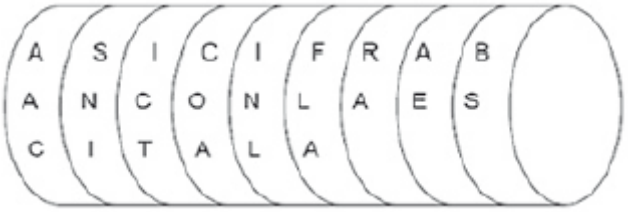
Los cifradores por transposición utilizan la técnica de permutación de forma que los caracteres del texto se reordenan mediante un algoritmo específico.

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.

La Scitala

En siglo V a.c. los lacedemonios, un antiguo pueblo griego, usaban el método de la scitala 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:



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.

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

Cifrado Vigenère

El cifrado Vigenère es un cifrado basado en diferentes series de caracteres o letras del cifrado César formando estos caracteres una tabla, llamada tabla de Vigenère, que se usa como clave. El cifrado de Vigenère es un cifrado polialfabético y de sustitución.

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

Mensaje: P A R I S V A U T B I E N U N E M E S S E

Clave: L O U P L O U P L O U P L O U P L O U P L

Criptograma: A O L X D J U J E P C T Y I H T X S M H P

6.2.2 Criptografía Moderna

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

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.

Criptografía Simétrica por Bloques

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.

Algunos de los sistemas criptográficos que utilizan esta filosofía son:

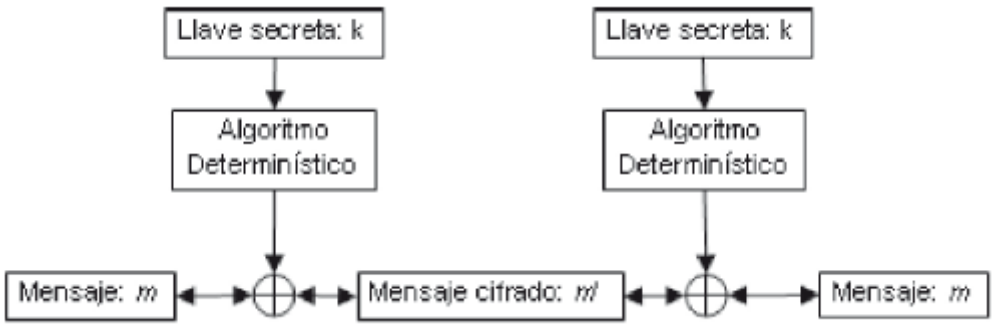
Algoritmo	Bloque (bits)	Llave (bits)	Vueltas
Lucifer	128	128	16
DES	64	56	16
Loki	64	64	16
CAST	64	64	8
Blowfish	64	Variable	16

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).

Criptografía Simétrica de Flujo

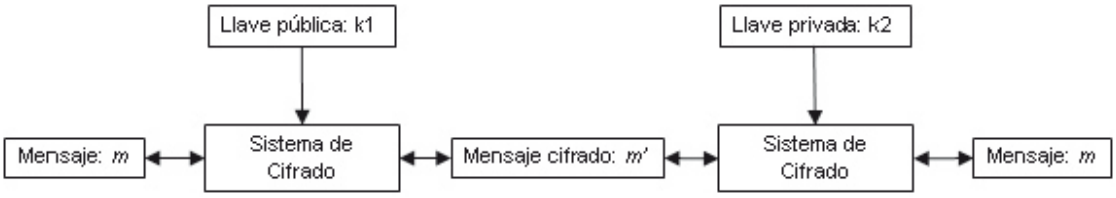
Este tipo de criptografía se basa en hacer un cifrado bit a bit, esto se logra usando la operación XOR, representada con Å. Se utiliza un algoritmo determinístico que genera una secuencia pseudoaletoria de bits que junto con los bits del mensaje se van cifrando utilizando a operación XOR.



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

Criptografía Asimétrica

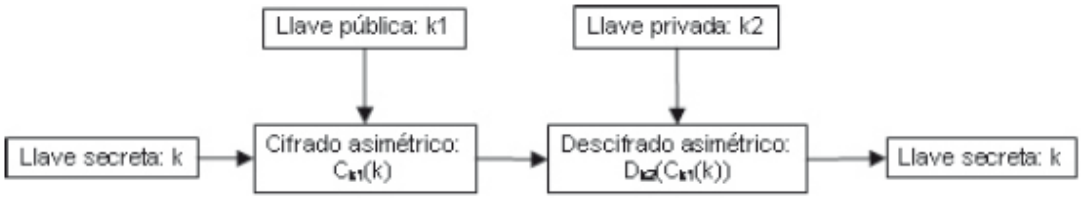
Si se observa la siguiente figura, que ilustra la idea de criptografía de llave pública, se puede ver claramente que no existe simetría en ella, ya que de un lado de la figura se cifra o descifra con una llave pública y en el otro lado con una privada. De este hecho es de donde la criptografía asimétrica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



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 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.



6.3 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

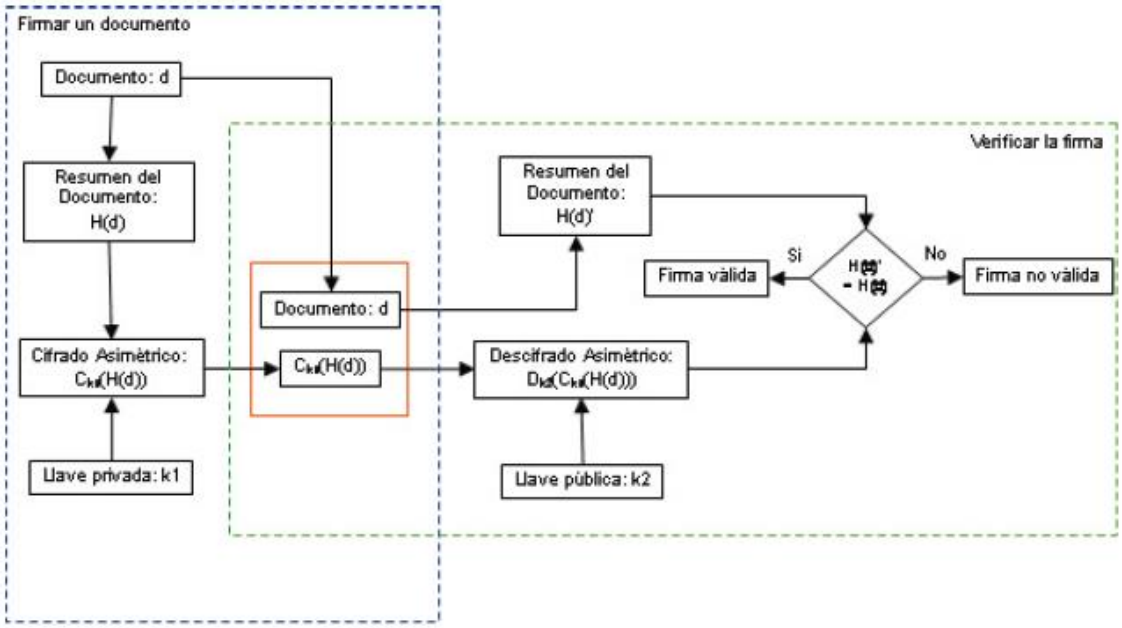
Una firma digital es un documento que permite garantizar la integridad de un documento y se puede relacionar de manera única al firmante con su firma, ya que realiza ésta con la llave privada y únicamente el firmante posee esa llave, esto se traduce en que se verifica la autenticidad del firmante.

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.

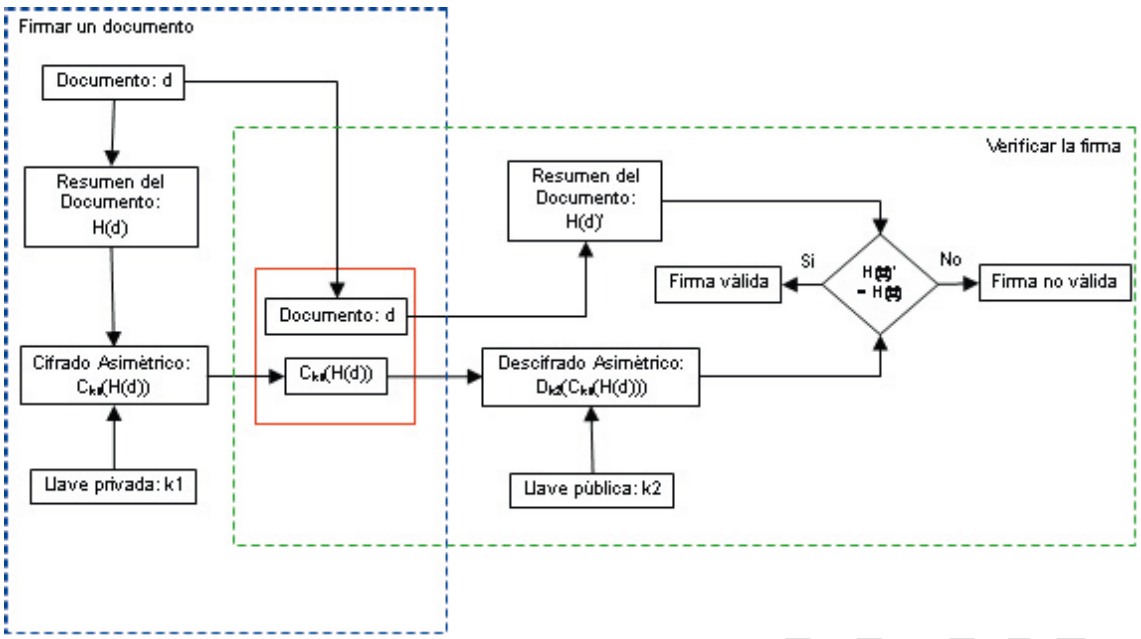
Ahora hay que verificar la firma, para eso se separan el documento d del resumen cifrado. Se descifra asimétricamente con la llave pública k2 del firmante el resumen cifrado Dk2(Ck1(H(d))) obteniéndose el resumen del documento original H(d). Se obtiene el resumen del documento enviado H(d)’ se comparan 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.



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.



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.

6.4 Seguridad en las Comunicaciones

En el pasado, Telnet ha sido el protocolo de inicio de sesión remoto en modo texto elegido en sistemas Linux y Unix. Lamentablemente, Telnet es sumamente pobre en características de seguridad. Así, en los últimos años SSH ha crecido en popularidad, y de hecho es la herramienta preferida de inicio de sesión remoto. SSH también puede manejar tareas de transferencia de archivos similares a las de FTP

6.4.1 Fundamentos de SSH

Linux soporta acceso remoto a través de varios servidores diferentes, como Telnet, Virtual Network Computing (VNC), e incluso X. Desafortunadamente, la mayoría de estos métodos sufren de una desventaja importante: la transferencia de todos los datos sobre la red en forma no codificada. Este hecho significa que cualquiera que pueda monitorizar el tráfico de red, puede capturar datos sensibles, a menudo incluyendo contraseñas.

SSH fue diseñado para cerrar esta brecha de seguridad empleando técnicas de cifrado fuerte para todas las partes de la conexión de red.

SSH encripta la contraseña y el intercambio de todas las transferencias de datos posteriores, por lo que es un protocolo mucho más seguro para el acceso remoto.

Además de cifrado, SSH proporciona características de transferencia de archivos y la capacidad de tunelizar otros protocolos de red, es decir, permitir que los protocolos no encriptados puedan enviar sus datos a través de una conexión SSH.

El principal inconveniente de SSH es que el cifrado y descifrado consumen tiempo de CPU.

Este hecho retrasa las conexiones SSH en comparación con las conexiones directas y puede degradar el rendimiento global del sistema.

Este efecto no es muy acusado, sobre todo en la transferencia de texto.

Si tunelizamos un protocolo que transfiere muchos más datos, como X, podemos ver una mayor caída de rendimiento al utilizar SSH.

Hay varios servidores SSH disponibles para Linux, pero el más popular con diferencia es el servidor OpenSSH (http://www.openssh.org). Este programa fue una de las primeras implementaciones abiertas del protocolo SSH, que fue desarrollado por SSH Communications Security (http://www.ssh.com), cuyo servidor se vende bajo el nombre de SSH Tectia.

OpenSSH, SSH Tectia, y otros productos SSH pueden interoperar entre sí, suponiendo que todos están configurados para soportar al menos un nivel común de protocolo SSH.

OpenSSH soporta los niveles de SSH 1.3, 1.5 y 2.0, con 2.0 siendo el nivel preferido, debido a vulnerabilidades conocidas en las versiones anteriores.

6.5 Seguridad en los Datos

SSH está diseñado para cifrar sesiones de inicio de sesión interactivo y transferencias de archivos. A veces, sin embargo, es deseable otro tipo de cifrado: Es posible que deseemos cifrar mensajes de correo electrónico o ficheros que se envíen a otra persona a través de otros medios. El E-mail nunca fue diseñado como una herramienta segura de transferencia de datos, y la mayoría de los mensajes de correo electrónico pasan a través de varios servidores de correo electrónico y routers. En cualquiera de estos puntos un cracker podría sniffar tráfico de correo electrónico y recopilar datos sensibles, como tarjetas de crédito o números de DNI.

La herramienta habitual para la encriptación de correo electrónico es el paquete GNU Privacy Guard (GnuPG o GPG; http://www.gnupg.org).

Este paquete es una re-implementación de código abierto del propietario Pretty Good Privacy (PGP).

Además de cifrar los mensajes completos, GPG nos permite firmar digitalmente mensajes. Utilizado de esta manera, los mensajes pueden ser leídos por destinatarios que no tienen el software GPG o las claves adecuadas, pero aquellos que disponen de estas herramientas pueden verificar que el contenido no ha sido manipulado.

En este tema haremos una práctica en la que utilizaremos GPG.