UT-6 CRIPTOGRAFIA

Contenido

Como asegurar la privacidad de la información

La información es poder. *Por ejemplo: los planos de un nuevo motor de coche eléctrico, la estrategia electoral de un partido político.* Todos son ejemplos de información que interesan a terceras personas.

Para sacar el máximo partido de esa información hay que compartirla. En todos estos casos el autor del documento es el emisor, se debe transferir algún soporte (disco, USB, servidor web, etc) y hacer llegar este soporte a un destino que es el receptor, utilizando un canal de comunicación (la empresa, mensajería, fax, internet, etc). En ese canal puede aparecer terceras personas con intención de interceptarlo, es este momento es cuando nos interesa la criptografía.

El objetivo de la criptografía es que en el intercambio de información no haya nadie que nos pueda coger el mensaje, la finalidad de la criptografía es la confidencialidad por lo que se han desarrollado técnicas para ocultar la información.

En nuestra era de la información y las comunicaciones necesitan cifrado porque cada vez existen más medios de almacenamiento y sobre todo más mecanismos de comunicación:

- **Voz.**-Mediante teléfono con tecnología analógica y digital. Así como aumento constante de videoconferencias
- **Mensajería Electrónica Breve,** como SMS, WhatsApp o como correo electrónica, buroFAX
- **Datos por línea digital.**- ADSL, Fibra óptica o inalámbrica: Wi-Fi, LTE, UMTS, etc
- **Apertura de las redes internas en la empresa.**- Para que puedan trabajar sus trabajadores utilizando VPN de teletrabajo. Sus clientes (acceso web) y otras empresas (VPN de empresas).

Todas estas conversaciones utilizan redes compartidas con otros usuarios que no somos nosotros y administradas por otras empresas que nos son la nuestra. Las operadoras de telecomunicaciones pueden darnos confianza y utilizando protocolos seguros además de aplicar cifrado en todas las partes.

Historia de la Criptografía

Cripto.- Escondido
Grafía.-Escritura

La criptografía es la ciencia que estudia la escritura oculta, es decir aquella que enseña a diseñar códigos secretos e interpreta mensajes cifrados.

La criptografía consiste en coger el documento original y aplicarle un algoritmo, cuyo resultado es un nuevo documento. Ese documento está cifrado y podemos mandarlo al destinatario que sabrá aplicar el algoritmo que recupera el documento original

Antecedentes Históricos

Siglo V a.C

Los espartanos utilizan una técnica llamada escítala para ocultar la comunicación.

El método consistía en enrollar una cinta sobre un bastón y posteriormente escribir el mensaje en forma longitudinal. Después la cinta se desenrollaba del bastón yero enviado mediante un mensajero; si éste ero atrapado por los enemigos, sólo obtendrían un conjunto de caracteres sin sentido. El receptor sólo podría interpretar el mensaje siempre y cuando tuviese un bastón similar al que se utilizó para ocultar el mensaje, es decir una vara con el mismo diámetro.

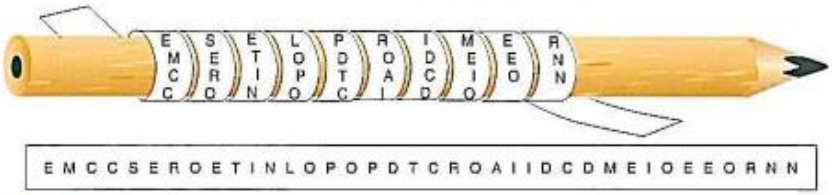


Fig. 4.1. *Escítala.*

Como podemos ver en la imagen, el mensaje es «es el primer método de encriptación conocido», pero en la cinta lo que se podría leer es «EMCCSEROETINLOPOPDTCROA IIDCDMEIOEEORNN».

Siglo II a.C

Los griegos utilizaron un método de sustitución de caracteres que se le atribuye a Polybios. Este método se encarga de sustituir una letra por un par de letras o números. Es el primer método de sustitución de caracteres.

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

Tabla 4.1. *Tabla cifrador de Polybios.*

El mensaje que queremos enviar es «el cifrador de Polybios es el primer cifrador por sustitución de caracteres», y el mensaje cifrado que enviaremos es «AECA ACBDBADBAAADCDDB ADAE CECDCAEDAB BDCDDC AEDC AECA CEDBBDCBAEDB ACBDBADBAAADCDDB CECDDB DCDEDCDDBDDDDEACBDCDCC ADAE ACAADBAAACDDAEDBAEDC» .

Caso práctico 1

Cómo cifrar con el cifrador de Polybios

Como hemos estudiado anteriormente, el cifrador de Polybios sustituía cada carácter del mensaje original por un par de letras o números. En el ejemplo anterior hemos cifrado la información mediante un par de letras, ahora lo vamos a hacer mediante números (Tabla 4.2).

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Tabla 4.2. *Tabla cifrador de Polybios.*

Recordamos el mensaje original: «el cifrador de Polybios es el primer cifrador por sustitución de caracteres».

El mensaje cifrado sería: 1531 1324214211143442 1415 3534315412243443 1543 1531 354224321542 1324214211143442 353442 434543442444451324343 3 1415 131142111344154215 43

Siglo I a.C

Los romanos desarrollaron el cifrador de Cesar que consistía en sustituir cada caracter por otro desplazando tres posiciones hacia la derecha el carácter original del alfabeto utilizado

Siglo XV

León Battista Alberti utiliza uno o más alfabetos cifrados y será en el siglo XVI cuando vigenere desarrollo la idea de Alberti y utiliza hasta 16 alfabetos cifrados. El cifrado se realiza combinando diferentes alfabetos

En la segunda guerra mundial se hace imprescindible el uso de máquinas para cifrar mensajes

http://goo.gl/NtBiQ

http://alt1040.com/2011/07/la-maquina-enigma-el-sistema-de-cifrado-que-puso-en-jaque-a-europa

TENER EN CUENTA LA PG : http://www.criptored.upm.es/thoth/

Son píldoras sobre criptografía muy interesante

Criptografía

El uso de la clave es indispensable en la criptografía.

Las claves son combinaciones de símbolos (letras, números, signos, símbolos, etc)

Por tanto, nuestra seguridad está expuesta a los **ataques de fuerza bruta** que consisten en probar todas las combinaciones posibles de símbolos, para evitar estos ataques se deben tomar las siguientes medidas a la hora de elegir una clave:

1. **Utilizar claves de gran longitud**, de manera que el atacante necesite de muchos recursos para cubrir el rango rápidamente.
2. **Cambiar regularmente la clave**, de esta forma si alguien quiere intentar cubrir todo el rango de claves limitamos el tiempo para hacerlo
3. **Utilizar todos los tipos de caracteres posibles**, una clave compuesta por solo números es más fácil de adivinar que la que está compuesta por la combinación de números y letras
4. **No utilizar palabras fácilmente identificables**, por ejemplo, palabras de diccionario, nombres propios, etc
5. **Intentar repetidos intentos fallido**s en un corto intervalo de tiempo, por ejemplo, la tarjeta del móvil se bloquea si se falla durante 3 intentos.

Las claves no son el único punto débil de la criptografía, también puede haber vulnerabilidades en el propio algoritmo, estas vulnerabilidades las estudia en criptoanálisis.

Clasificación de los métodos de criptología o cifrado

1. **Sistemas de transposición**.- Consiste en descolocar el orden de las letras, silabas o conjunto de letras. En función del número de transposiciones de clasifican en:
    a. Transposición simple.- Donde el texto se somete a una sola transposición.
    b. Transposición doble o múltiple.- Es cuando se realiza una segunda o tercera transposición sobre un texto cifrado mediante transposición simple, con esto se consigue mayor seguridad.
2. **Sistema de sustitución**.- Se remplazan letras del alfabeto por otras o por un conjunto de ellas y pueden ser:
    a. Literal.- Se sustituyen por letras
    b. Numéricas.- se sustituyen por números
    c. Esteganografia.- Cuando se oculta un mensaje tras una imagen o un sonido.

Cifrado/descifrado de la información.

- **Métodos para asegurar la confidencialidad:**
    - **Protección del algoritmo**
    - **Protección de la clave.**
- **Tipos de algoritmos:**
    - **En función de la gestión de la clave:**
        - **Simétrico**
        - **Asimétrico**
        - **Hibrido**
    - **En función del método de cifrado**
        - **En bloque:DES AES,etc**
        - **De flujo: A5,RC4,etc**
- **Criterios de elección**
    - **Algoritmos utilizados en función de la capa OSI:**
        - **Nivel de enlace**
            - **WEP**
            - **WAP/WAP2**
        - **Nivel de red**
            - **IPSEC**
        - **Nivel de transporte**
            - **SSL**
            - **TLS**

- **Nivel de aplicación**
  - **Mensajería**
  - **Comunicación con base de datos**
  - **etc**

Criptografia Simétrica, asimétrica e hibrida

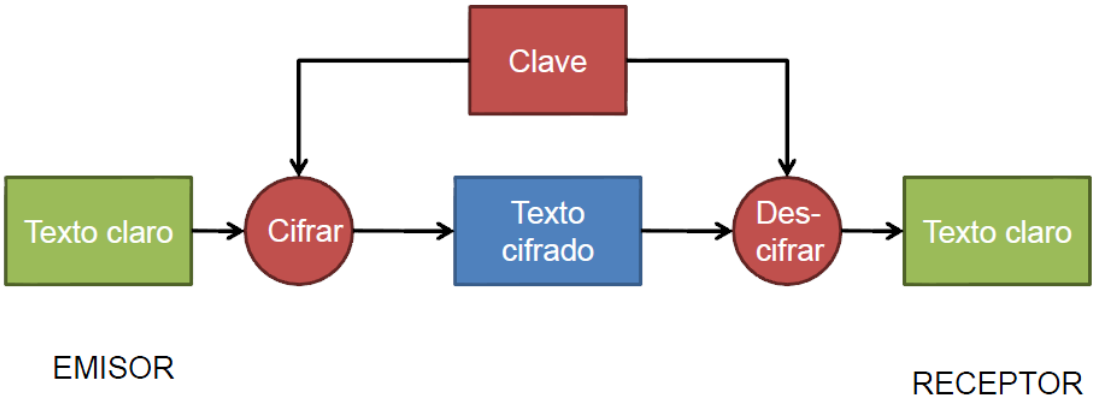
Criptografia Simétrica

También denominada clave simétrica o privada

Esta utiliza la misma clave tanto para el proceso de cifrado como el descifrado (las dos partes que se comunican deben ponerse de acuerdo sobre la clave a usar).

Todos los algoritmos, desde la antigüedad hasta los años 70 eran simétricos. Por ejemplo, el algoritmo DES, 3DES, AES, IDEA.

Un ejemplo de criptografía simétrica es la autenticación de un móvil GSM, ya que sabe que es nuestro número, aunque no metamos la tarjeta SIM en otro teléfono.



Problemas en este sistema de cifrado:

- El problema es el intercambio de las claves entre el emisor y el receptor, ya que en la comunicación puede ser no aceptadas.
- Para el atacante es más fácil interceptar las claves en este tipo de comunicación
- La gestión de las claves almacenadas ya que el número de claves que se necesitan se calcula teniendo en cuenta el número de personas diferentes con la siguiente formula.

N*(N-1)/2
Calculo de número de claves que tengo que hacer

N.- número de personas

Las ventajas que ofrece:

- Eficiente (los algoritmos utilizados son muy rápidos).

Ejemplos de algoritmos simétricos: DES, Triple DES (3DES), IDEA, AES, BLOWFISH, RC4, RC5

Usos principales (aplicaciones):

- Transmisión de datos sobre un canal inseguro (emails, …).
- Almacenamiento de datos (ficheros, particiones, bases de datos).

Método de ataque:

- Fuerza bruta
- Para que el ataque sea computacionalmente irrealizable se recomienda una longitud mínima de 128 bits de clave.

Sistemas de cifrado con clave simétrica:
http://www.criptored.upm.es/intypedia/video.php?id=criptografia-simetrica&lang=es

Criptografia Asimétrica o Clave Pública

Consiste en que cada una de las partes involucradas en la comunicación debe tener una pareja de claves.

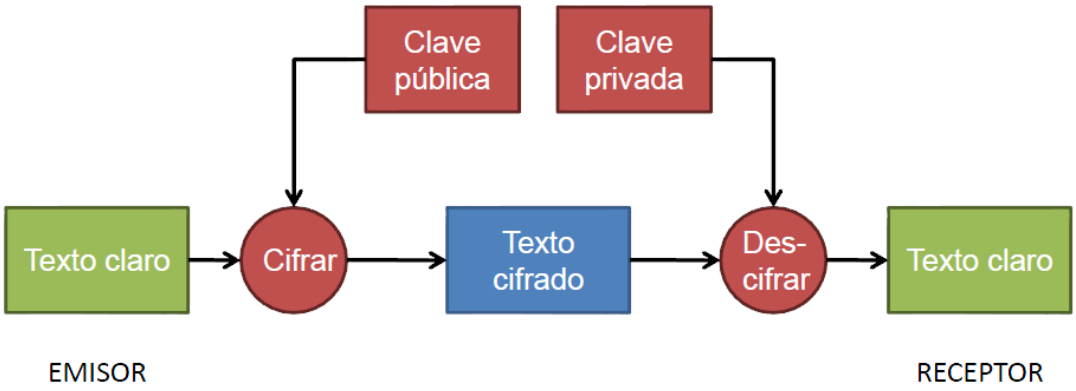
- Una clave privada que solo tiene 1 propietario.
- Una clave pública que va a ser compartida con el resto de los usuarios.

Esta pareja de claves es complementaria, es decir con una se cifra y con otra se descifra.

Estas claves se obtienen mediante algoritmos matemáticos complejos, *por ejemplo: MD5, SHA*

Para cifrar un mensaje el emisor utilizara la clave pública del receptor y a su vez, el receptor utilizara su clave privada para descifrar el mensaje

Cuando el emisor quiere hacer llegar un mensaje confidencial al receptor, primero consigue la clave pública del receptor. Con esa clave y el documento original aplica el algoritmo asimétrico. El resultado es un documento cifrado que puede enviar al receptor por cualquier canal. Cuando el mensaje cifrado llega al receptor, el recupera el documento original aplicando el algoritmo asimétrico con su clave privada.



Ventajas de la criptografia asimétrica

1. El mensaje se cifra con una clave y se descifra con otra
2. No necesitamos canales seguros para comunicar la clave que utilizaremos en el cifrado. Podemos adjuntarla a nuestros correos, añadirla al perfil de nuestras redes sociales, etc
3. No hay desbordamiento en el tratamiento de claves y canales, si somos 9 empleados solo necesitamos 9 claves y un solo canal

Desventajas de la criptografia asimétrica:

1. **Son poco fiables al darle tanta prioridad a la clave,** la longitud de dicha clave y la combinación de diferentes caracteres para que sea segura obliga a que se ralentice bastante el proceso de encriptación y el mensaje cifrado ocupa más espacio
2. **Hay que proteger la clave privada**, si la guardamos en un disco duro se puede obtener fácilmente. Por este motivo las claves privadas se guardan en un fichero llamado ***Keyring*** (archivo de llaves o llavero). Este fichero está protegido mediante un cifrado simétrico. Es decir, para usar la clave privada hay que introducir otra clave que descifra el llavero y permite leerla. Necesitamos también una segunda medida de protección de la clave privada que es la copia del llavero. De estas claves debemos de hacer copias de seguridad
3. Hay que transportar la clave privada, por lo que tenemos que transportar también el llavero, y esto supone un riesgo.

La **solución** más común a los problemas para proteger la clave privada es emplear una tarjeta inteligente que contiene un chip electrónico hay dos tipos:

a. **Tarjeta de memoria**, que se limita a almacenar el llavero, cuando se introduce el lector el ordenador hace una copia temporal del llavero y trabaja con el introduciendo la clave simétrica (es mas peligrosa)
b. **Tarjeta procesadora**.- es más fiable ya que las claves nunca salen de la tarjeta (tarjeta sim de los móviles)

- Las **tarjetas inteligentes** se pueden clasificar en:
  - **Tarjetas de contacto**, el lector necesita tocar los contactos metálicos del chip para interactuar (se utiliza en los bancos, para sacar dinero)
  - **Tarjetas sin contactos**, se utiliza tecnología inalámbrica (p.e. las tarjetas que utilizamos en el transporte)

Este cifrado ofrece confidencialidad, autentificación y no repudio

Las ventajas que ofrece: clave privada no se transmite y es suficiente que cada usuario tenga su clave doble pública-privada.

Usos principales (aplicaciones):

- Distribución de claves secretas (SSL/TLS, SSH, ...).
- Firma digital.

Sistemas de cifrado con clave asimétrica:
http://www.criptored.upm.es/intypedia/video.php?id=criptografia-asimetrica&lang=es

Unas de las herramientas para crear claves en software son **GPG** (linux) y PGP (windows)

Criptografia Híbrida

La desventaja de la criptografía de **clave pública** es la lentitud del proceso de cifrado y descifrado, que obedece tanto a la complejidad de los métodos utilizados como a la longitud de las claves.

La desventaja de la criptografía de **clave privada** es el intercambio de claves

¿Por qué no usar únicamente criptografía asimétrica?

- El cifrado y descifrado es más lento y costoso en CPU que si se usa un algoritmo de criptografía simétrica.

¿Por qué no usar únicamente criptografía simétrica?

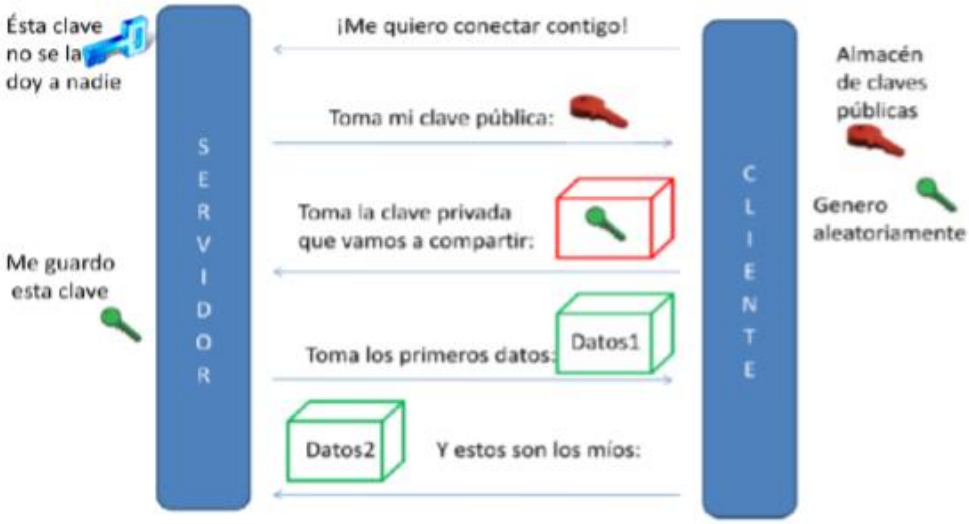
- Es problemático intercambiar la clave.

Lo ideal sería utilizar criptografía de clave privada para intercambiar mensajes, pues estos son más pequeños y además el proceso es rápido, y utilizar criptografía de clave pública para el intercambio de las claves privadas.

A modo de **ejemplo** describiremos un proceso de comunicación seguro:
Julia y Gonzalo tienen sus pares de claves respectivas:

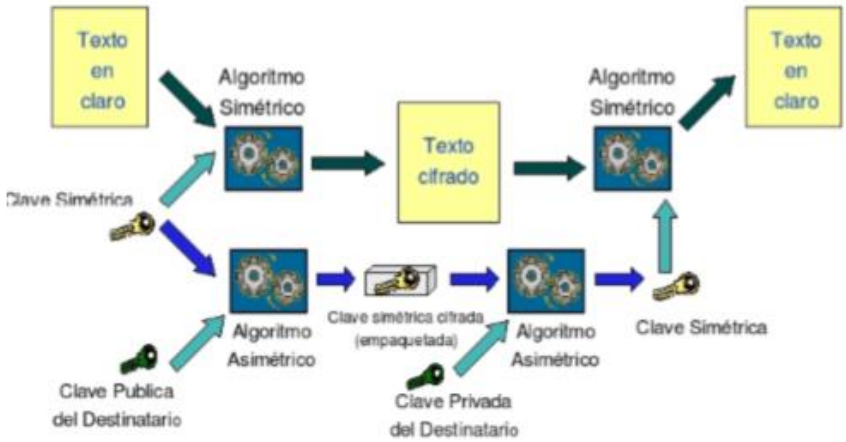
1) Julia escribe un mensaje a Gonzalo. Lo cifra con el sistema de criptografía de clave simétrica.
2) La clave que utiliza se llama clave de sesión y se genera aleatoriamente. Para enviar la clave de sesión de forma segura, ésta se cifra con la clave pública de Gonzalo, utilizando por lo tanto criptografía de clave asimétrica.
3) Gonzalo recibe el mensaje cifrado con la clave de sesión y ésta misma cifrada con su clave pública. Para realizar el proceso inverso, en primer lugar utiliza su clave privada para descifrar la clave de sesión.
4) Una vez ha obtenida la clave de sesión, ya puede descifrar el mensaje.

Otro ejemplo: servidor seguro que se conecta con cliente



Ejemplo:

1) El cliente se conecta al servidor.
2) El servidor envía su clave pública.
3) El cliente verifica que la clave es realmente del servidor.
4) El cliente genera una clave simétrica, la cifra con la clave pública del servidor y se la envía.
5) El servidor recibe la clave simétrica y la descifra con su clave privada.
6) Los dos tienen la clave privada para intercambiar información cifrada



Algoritmos que se utilizan en las criptografías

Algoritmo son métodos que se utilizan para transformar texto plano en texto cifrado.

Cifrado es el proceso de convertir el texto plano en texto ilegible (encriptado). Por lo general el algoritmo se basa en una clave secreta que adapta el algoritmo de cifrado para cada uso distinto.

La fortaleza del cifrado del documento va a depender del tipo de clave.

Los algoritmos de cifrado se clasifican en:

- **Cifrado en bloque**.- se ocupan de dividir el texto en bloques o grupos de bit de tamaño fijo y se cifran de forma independiente. Primero se cifra el documento y segundo se transmite el mensaje
- **Cifrado en flujo**.- se realiza bit a bit o byte a byte. Se utiliza cuando hay que transmitir información privada según se va generando.

Los diferentes algoritmos de cifrado para la criptografia privada son:

- DES
- 3DES
- RSA

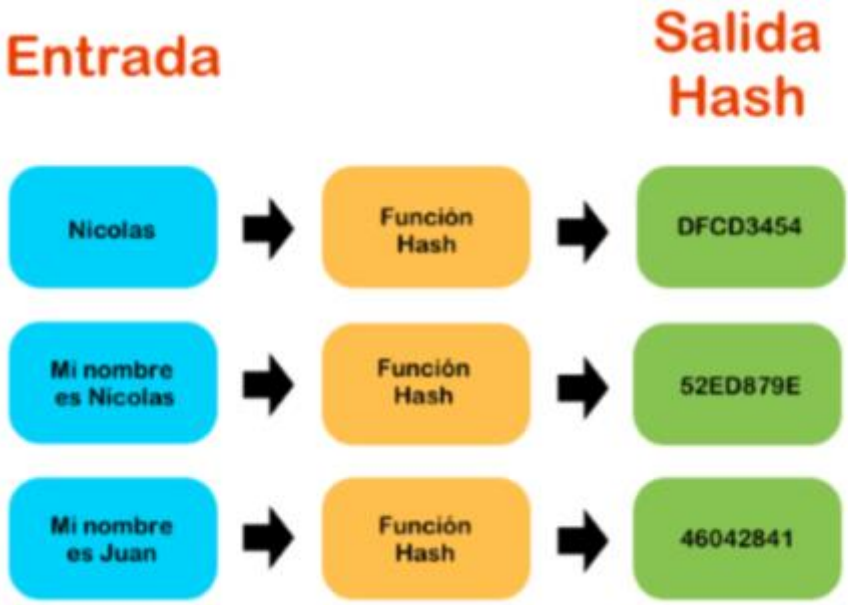
Para la criptografia pública son:

- RSA
- DH

Función Resumen o HASH

Son funciones que asocian un documento a un número. Para obtener el valor resumen de un documento se emplean algoritmos matemáticos complejos. Esta función resumen tiene que ser única para cada documento y dos documentos no pueden tener una función resumen igual.

Una función hash es una función que toma un mensaje de tamaño arbitrario como entrada y produce un valor de salida de una longitud fija (típicamente 16 ó 20 bytes). Una función hash “nunca” genera dos valores de salida iguales



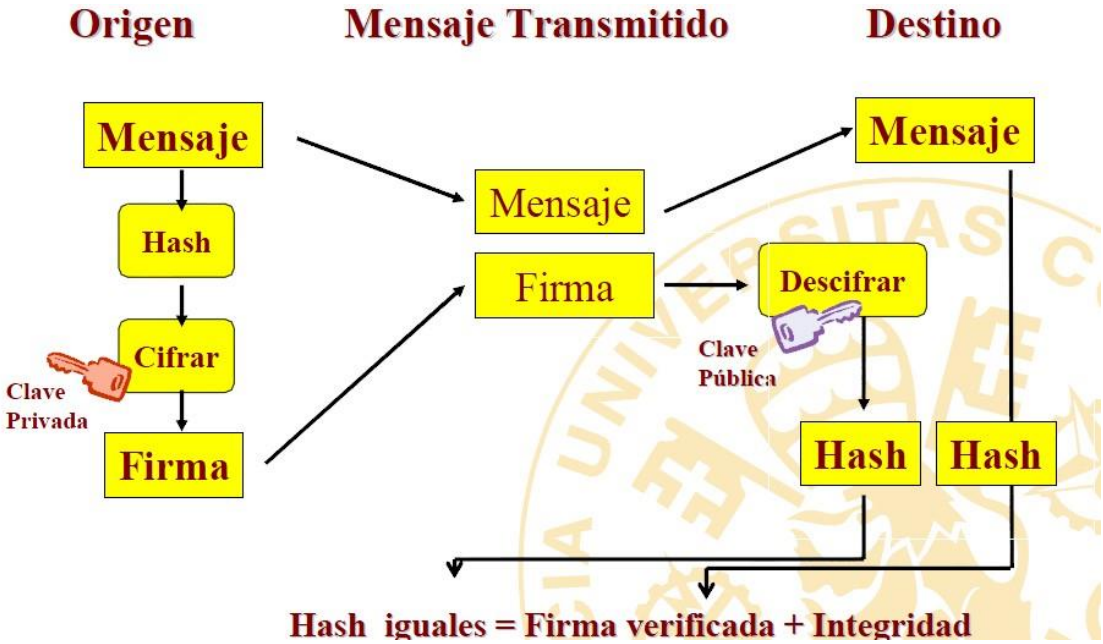
Atributo	Clave simétrica	Clave asimétrica
Años en uso	Miles	Menos de 50
Uso principal	Cifrado de grandes volúmenes de datos	Intercambio de claves; firma digital
Estándar actual	DES, Triple DES, AES	RSA, Diffie-Hellman, DSA
Velocidad	Rápida	Lenta
Claves	Compartidas entre emisor y receptor	Privada: sólo conocida por una persona Pública: conocida por todos
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La clave pública se comparte por cualquier canal La privada nunca se comparte
Longitud de claves	56 bits (vulnerable) 256 bits (seguro)	1024 – 2048 (RSA) 172 (curvas elípticas)
Servicios de seguridad	Confidencialidad Integridad Autenticación	Confidencialidad Integridad Autenticación, No repudio

Firma digital

La firma digital es una de las principales ventajas de la criptografía de clave pública o asimétrica. Con esta firma permite al receptor verificar la autenticación del mismo y la integridad de los datos.

La firma digital es el resultado de cifrar con clave privada el resumen de los datos a firmar utilizando algoritmos HASH.

Proceso:

- Calcular el valor resumen del documento con algoritmo SHA
- El valor resumen calculado se cifra con la clave privada de nuestra pareja de claves el resultado de este valor se conoce como firma digital
- 

Dos documentos distintos firmados digitalmente por una misma persona tendrán firmas digitales diferentes

Comprobación de la firma digital

1. La firma se descifra con la clave pública y se obtiene el valor resumen
2. Para obtener el valor resumen del documento se utiliza el mismo algoritmo que se empleó en el proceso de cifrado
3. Se compara los dos valores obtenidos y si coinciden se verifica que es correcto

Con la firma digital se consigue

- Integridad
- Autenticación
- no repudio

Proceso completo:

1. el emisor aplica la función HASH para generar el resumen
2. el emisor toma su clave privada para aplicar el algoritmo asimétrico al documento resumen. El resultado es un documento cifrado
3. el emisor toma la clave pública del receptor para aplicar el algoritmo asimétrico al documento original y al documento resumen. El resultado es un documento conjunto cifrado que se envía al receptor. El receptor utiliza su clave privada

para descifrar los documentos y la clave pública del origen para comprobar su firma

Certificados digitales

Es un archivo que puede emplear un software para firmar digitalmente ficheros o mensajes como por ejemplo un correo electrónico y verifica la identidad de la persona que firma.

Hay certificados digitales que identifican a persona a organismos y contiene información sobre

1. nombre y dirección de correo electrónico
2. fecha de inicio y final de validez de la clave publica
3. Autorización certificadora

El certificado digital garantiza la unicidad de las claves y se suele recurrir a soportes como tarjetas, que dan mayor seguridad ya que estas suelen estar protegidas con un PIN. La casa de la moneda y timbre es la que emite los certificados
El certificado digital puede ser instalado en el sistema operativo, en aplicaciones (navegadores) o clientes de correo.
La extensión del certificado con clave privada suele ser un .TFX o .P12 mientras que el certificado que no tiene clave privado solo la pública, suele ser de extensión .CER o .CRT.
http://www.fnmt.es/ceres

PKI (Infraestructura de Clave Pública)

Se podrá tener confianza en el certificado digital si este está avalado por una tercera persona en la que confiamos, la forma en la que la tercera persona avalara es mediante la firma digital.

La base de definición de PKI es la confianza basada en terceros

Criptografía – DNI electrónico

El Documento Nacional de Identidad (DNI), emitido por la Dirección General de la Policía (Ministerio del Interior), es el documento que acredita, desde hace más de 50 años, la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular.

Documento Nacional de Identidad electrónico (DNIe), similar al tradicional y cuya principal novedad es que incorpora un pequeño circuito integrado (chip), capaz de

guardar de forma segura, mediante medidas específicas de seguridad para impedir su falsificación, información en formato digital. La información contenida es la siguiente:

- Un certificado electrónico para autenticar la personalidad del ciudadano.
- Un certificado electrónico para firmar electrónicamente, con la misma validez jurídica que la firma manuscrita.
- Certificado de la Autoridad de Certificación emisora.
- Claves para su utilización.
- La plantilla biométrica de la impresión dactilar

Para la utilización del DNI electrónico es necesario contar con determinados elementos:

- Hardware específico: lector de tarjetas inteligentes que cumpla el estándar ISO-7816. Existen distintas implementaciones, bien integrados en el teclado, bien externos (conectados por ejemplo vía USB).
- Software específico: mediante controladores o módulos criptográficos que permitan el acceso al chip de la tarjeta y, por tanto la utilización de los certificados contenidos en él. En Windows es el servicio Cryptographic Service Provider (CSP), y en los entornos GNULinux o MAC el módulo criptográfico se denomina PKCS#11.

https://www.dnielectronico.es/PortalDNIe/