Arquitectura de Comunicaciones

Criptografía

Tipos de Ataques

Ataques Pasivos

- Escucha de las transmisiones para obtener información
- Divulgación del contenido del mensaje
- Análisis de trafico:
  - Si se conoce la frecuencia y longitud de un mensaje (aunque este cifrado) se puede descubrir el contenido.
- Difíciles de detectar
- Se pueden Prevenir

Tipos de Ataques

Ataques Activos

- Enmascaramiento
  - Una entidad pretende ser otra
- Repetición
- Modificación de los mensajes
- Denegación de un servicio (DDOS)
- Fácil de detectar
  - Por lo general la detección es disuasiva
- Difícil de Prevenir

DEFINICIONES

La criptología (del griego criptos=ocultos y logos=tratado, ciencia), se compone de:

- *Criptografía: Procedimientos para cifrar, o enmascarar información de carácter confidencial. Surge como una necesidad, ya que el desarrollo de las comunicaciones electrónicas hace posible la transmisión y almacenamiento de información confidencial que es necesario proteger.*

- *Criptoanálisis: Procedimientos para descifrar y recuperar la información original.*

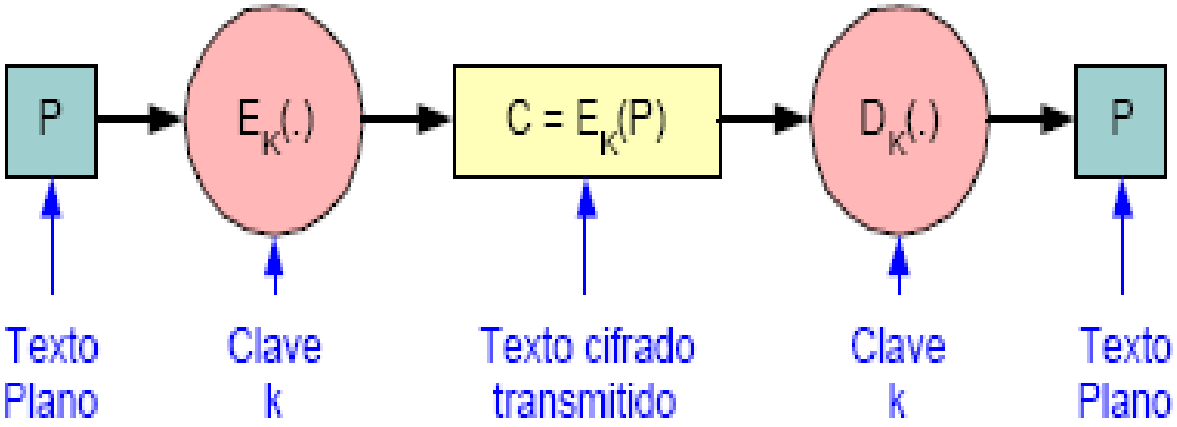
FINALIDAD DE LA CRIPTOGRAFÍA

Un sistema criptográfico ideal será aquel que ofrezca un descrifrado imposible pero un encriptado sencillo.

La finalidades son:

- Confidencialidad. Es decir, garantiza que la información sea accesible únicamente a personal autorizado.
- Autenticación. Es decir proporciona mecanismos que permiten verificar la identidad del comunicador.
- Integridad. Es decir garantiza la corrección y completitud de la información.
- Vinculación. Permite vincular un documento o transacción a una persona o un sistema de gestión criptográfico automatizado.

PROCESO CRIPTOGRAFICO



El cifrado es el proceso de convertir el texto plano en caracteres ilegibles, denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave: información secreta que adapta el algoritmo de cifrado para cada uso distinto.

CLAVES – Keyspace

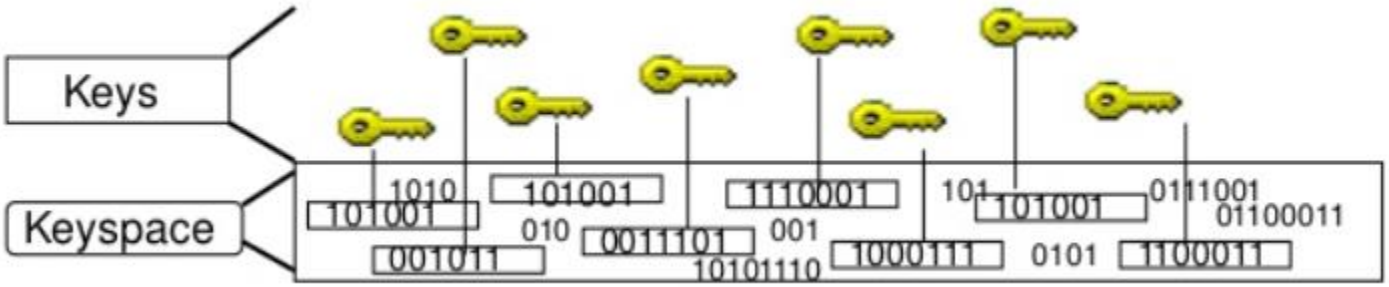
- Keyspace (Espacio de llave)

Es el rango de posibles valores que pueden ser usados para una llave.

Si un algoritmo permite una longitud de 2 bits, el espacio será

$$4\ (2^2 = 4) \rightarrow \quad 00 \quad 01 \quad 10 \quad 11$$

Cuando mayor es el keyspace mas cantidad de llaves aleatorias pueden ser utilizados en un algoritmo aleatorio



METODOS DE CIFRADO

- Sustitución:

Funcionamiento:
- **Reemplaza** cada carácter por otra.
- La **clave** especifica el tipo de sustitución.

M	U	R	C	I	E	L	A	G	O
0	1	2	3	4	5	6	7	8	9

Ej: COMO ESTAS → 39095ST7S

METODOS DE CIFRADO

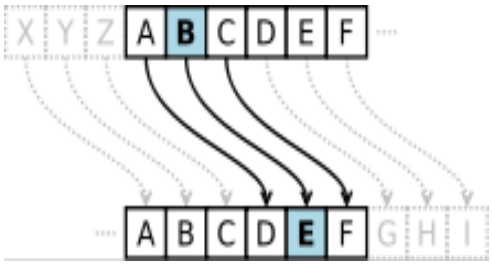
- Cifrado Cesar (Sustitución):

Funcionamiento:

- **Reemplaza** cada letra del alfabeto por otra más adelante en el alfabeto. Siempre a la misma distancia.
- La **clave** especifica la distancia.

Ejemplo:

Clave de sustitución: 3



Texto plano: SOPA
Texto cifrado: VRSD

Tipo de ataque : Análisis de frecuencia

METODOS DE CIFRADO

- Cifrado de transposición o permutación:
  Permuta o reordena los caracteres del texto plano.

  Ejemplo:

  Texto plano: ESTE ES UN MENSAJE DE PRUEBA
  Texto cifrado: EUAR SNJU TMEE EEDB ENEA SSP

  E S T E E S
  U N M E N S
  A J E D E P
  R U E B A

Tipo de ataque : Análisis de frecuencia

TIPOS DE CIFRADO SEGÚN SUS CLAVES

Una vez que el emisor y receptor acuerdan que algoritmo de cifrado usar, se distinguen dos tipos de cifrado:

- Cifrado **simétrico**:

Si la clave de cifrado y descifrado es la misma.

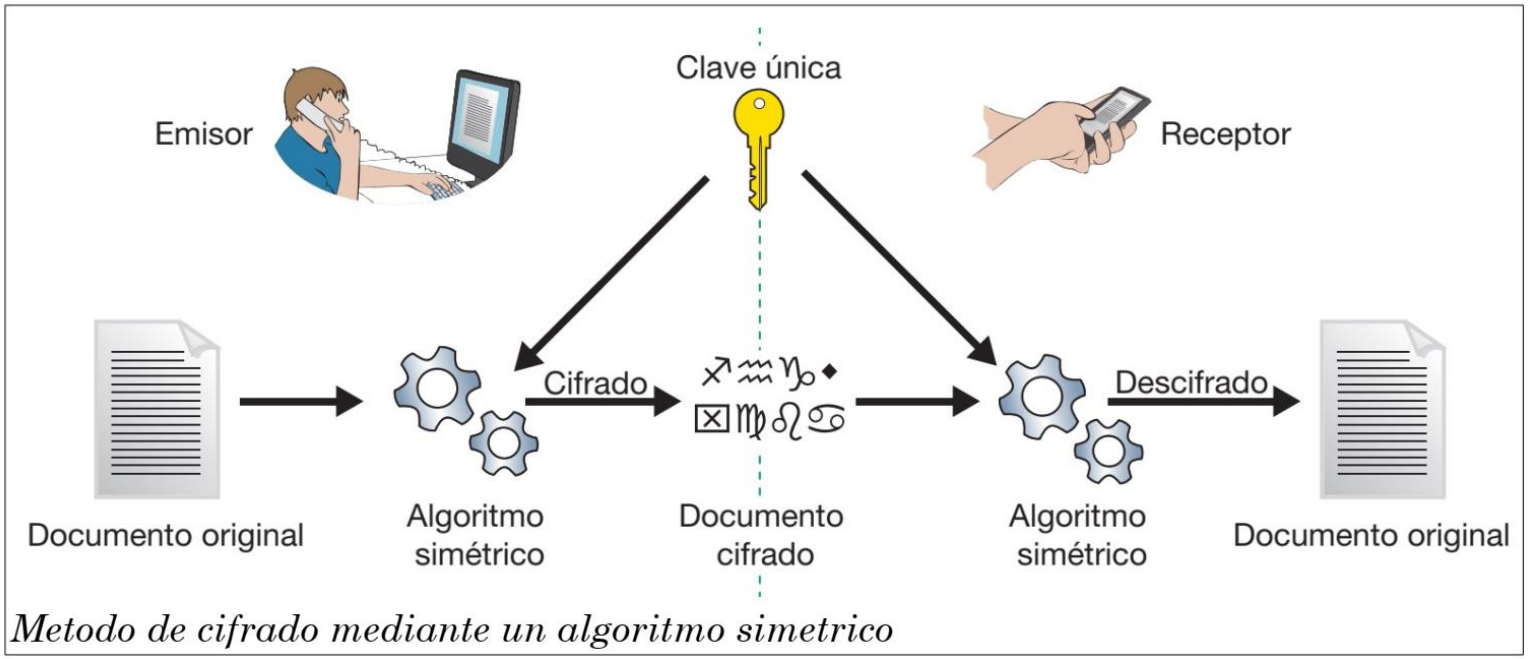
- Cifrado **asimétrico**:

Se hace uso de dos claves distintas:

Pública: Generalmente para cifrar.
Privada: Generalmente para descifrar.

CIFRADO SIMÉTRICO

La criptografía simétrica solo utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente.



Metodo de cifrado mediante un algoritmo simetrico

La posible intercepción de la clave es el punto débil de este sistema.

ALGORITMOS SIMÉTRICOS

- DES (Data Encryption Standard)
- 3DES
- IDEA (International Data Encryption Algorithm)
- AES (Advance Encryption Standard, Rijndael)
- Blowfish
- CAST 128
- RC2 (Cifrador de bloque permite de 1 a 2048 bits)
- RC4
- RC5

ALGORITMO AES

AES es un algoritmo de cifrado por bloques, inicialmente fue diseñado para tener longitud de bloque variable pero el estándar define un tamaño de bloque de 128 bits, por lo tanto los datos a ser encriptados se dividen en segmentos de 16 bytes (128 bits) y cada segmento se lo puede ver como un bloque o matriz de 4x4 bytes al que se lo llama estado.

Por ser simétrico, se utiliza la misma clave para encriptar como para desencriptar, la longitud de la clave puede ser de 128, 192 o 256 bits según especifica el estándar, esto permite tres implementaciones conocidas como AES-128, AES-192 y AES-256

CIFRADO ASIMÉTRICO

La criptografía asimétrica se basa en el uso de **dos claves**: **la pública** (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y **la privada** (que no debe de ser revelada nunca).

ALGORITMOS ASIMÉTRICOS

- RSA (Rivest/Shamir/Adleman) del MIT
- DSS
- ELGAMAL (Basado en aritmética exponencial y modular)

Usos:

Autenticación

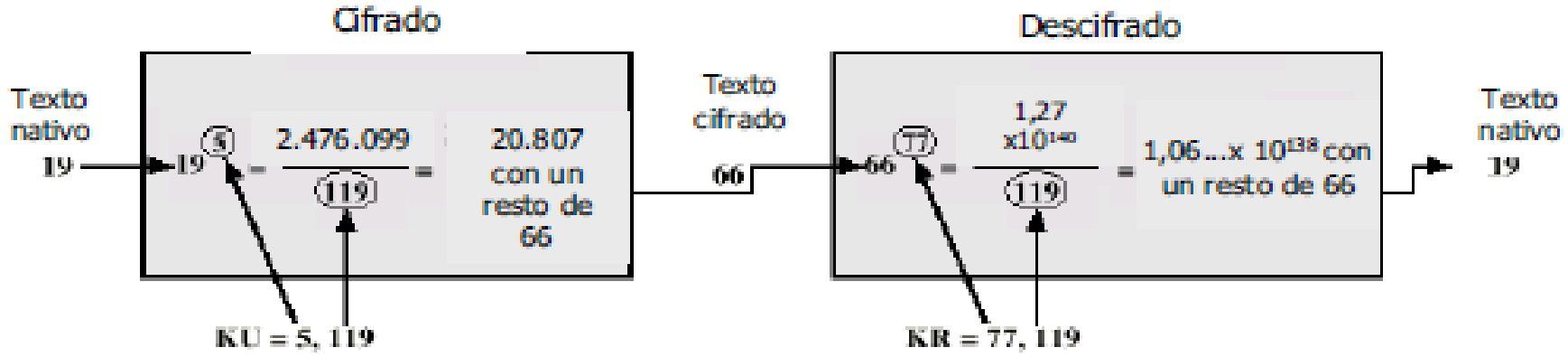
Firma digital

Intercambio de claves

ALGORITMO RSA

RSA – Rivest, Shamir y Adleman (1977)

- Algoritmo de criptografía mas usado a nivel mundial.
- Se utiliza para cifrar y firmar digitalmente.
- Las claves se basan en el producto de dos números primos muy grandes (Potencia de 300 o mas).
- Utiliza el esquema de clave publica y privada.



Comparativa entre Simétrica y Asimétrica

	Simétrico	Asimétrico
Más seguro		X
Más rápido	X	
Número de claves	N*(N-1)	2*N
Problema más significativo	Distribución de claves	Velocidad

Para combinar ambos sistemas (seguridad y velocidad), se utilizan sistemas híbridos.

SISTEMAS HÍBRIDOS

Este sistema es la unión de las ventajas de los dos anteriores, debemos de partir que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico es lento.
El proceso para usar un sistema criptográfico híbrido es el siguiente (para enviar un archivo):

- Generar una clave pública y otra privada (en el receptor).
- Cifrar un archivo de forma síncrona.
- El receptor nos envía su clave pública.
- Ciframos la clave que hemos usado para encriptar el archivo con la clave pública del receptor.
- Enviamos el archivo cifrado (síncronamente) y la clave del archivo cifrada (asíncronamente y solo puede ver el receptor).

SISTEMAS HÍBRIDOS

Ejemplos que combinan la **utilización de los métodos de criptografía de llave única y de llaves pública y privada** son las conexiones seguras, establecidas entre el browser de un usuario y una web, en transacciones comerciales o bancarias vía Web.

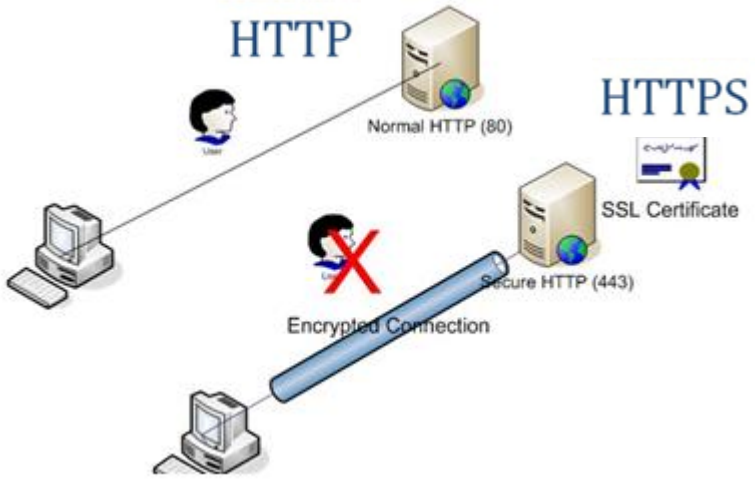
Estas conexiones seguras vía Web utilizan el método de criptografía de llave única, implementado por el protocolo **SSL (Secure Socket Layer).** El browser del usuario necesita informar a la web cual será la llave única utilizada en la conexión segura, antes de iniciar una transmisión de datos sigilosos.

PROTOCOLO SSL/TLS

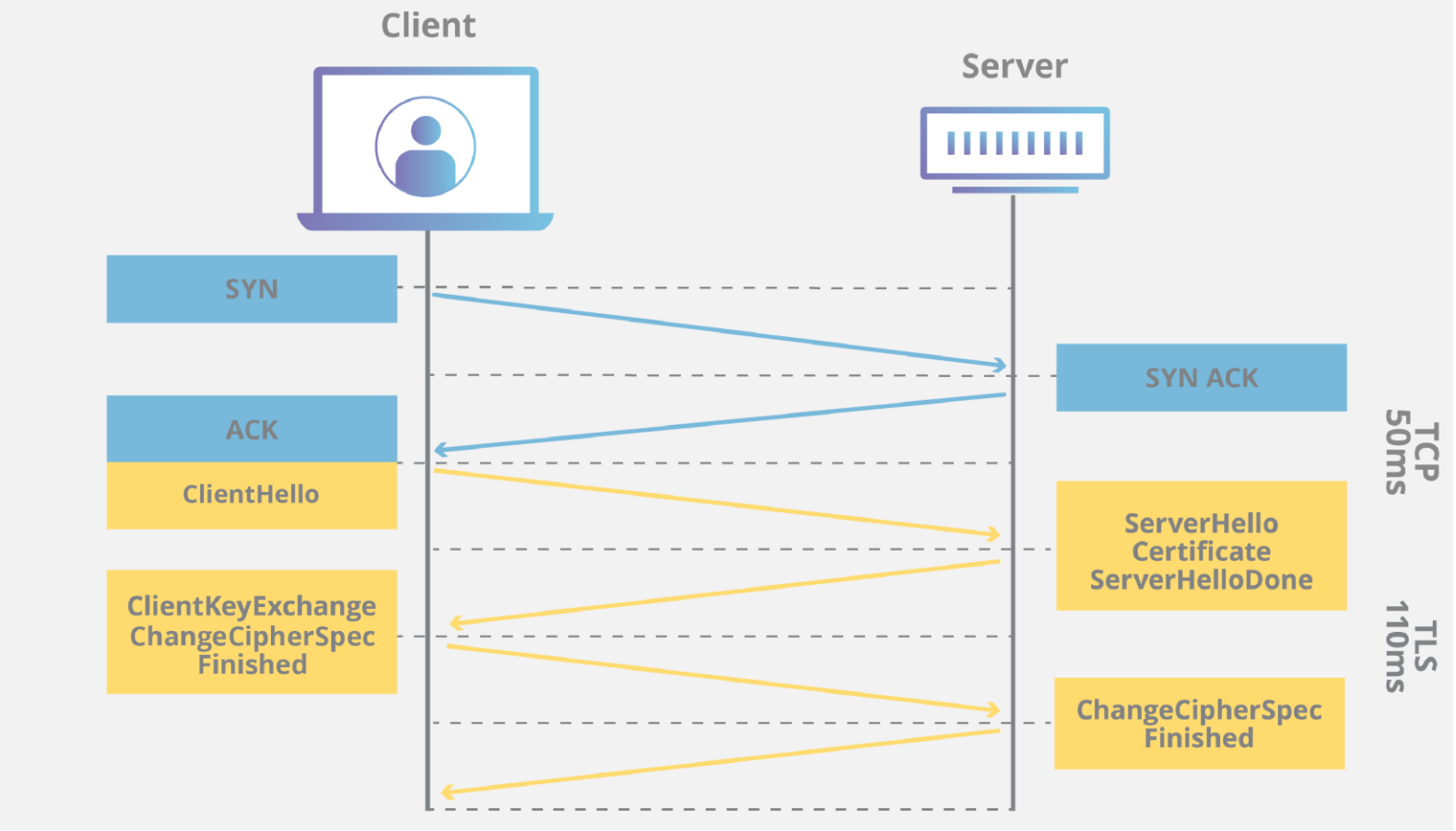
El protocolo SSL, "Secure Socket Layer" (en español, capa de puertos seguros), es el predecesor del protocolo TLS "Transport Layer Security" (Seguridad de la Capa de Transporte, en español).
Se trata de protocolos criptográficos que proporcionan privacidad e integridad en la comunicación entre dos puntos en una red de comunicación. Esto garantiza que la información transmitida por dicha red no pueda ser interceptada ni modificada por elementos no autorizados, garantizando de esta forma que sólo los emisores y los receptores legítimos sean los que tengan acceso a la comunicación de manera íntegra.

HTTPS - SSL

El browser obtiene la llave pública del certificado de la institución que mantiene la web. Entonces, utiliza esta **llave pública para codificar y enviar un mensaje a la web,** contiendo la llave única a ser utilizada en la conexión segura. La web utiliza su **llave privada para decodificar el mensaje** e identificar la llave única que será utilizada.



TLS/SSL Handshake



TIPOS DE CIFRADO SEGÚN SUS ALGORITMOS

Según el tratamiento del mensaje se dividen en:

- Cifrado en bloque (DES, IDEA, RSA, AES)
- Cifrado en flujo (A5, RC4 (River Cipher #4), SEAL) cifrado bit a bit según el tipo de claves

COSTO-TIEMPO PARA ENCONTRAR LA CLAVE

Cost	40	56	64	80	112	128
100 K	2 secs	35 hours	1 year	70,000 yrs	10^{14} yrs	10^{19} yrs
1 M	.2 secs	3.5 hours	37 days	7000 years	10^{13} yrs	10^{18} yrs
10 M	.02 secs	21 mins	4 days	700 years	10^{12} yrs	10^{17} yrs
100 M	2 millisecs	2 mins	9 hours	70 years	10^{11} yrs	10^{16} yrs
1 B	.2 millisec	13 secs	1 hour	7 years	10^{10} yrs	10^{15} yrs

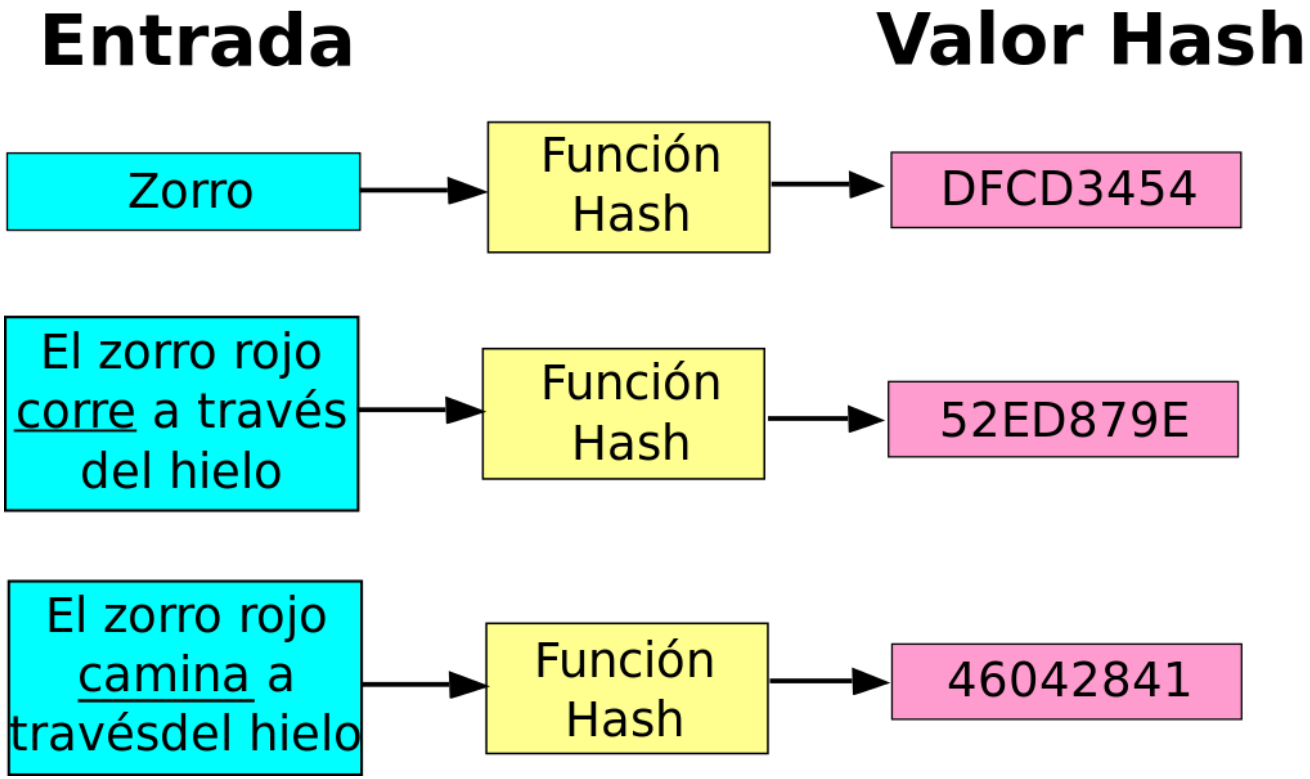
HASHING (Digest)

El "hashing" alude al proceso de generar una salida de extensión fija, a partir de una entrada de extensión variable. Esto se logra mediante el uso de unas fórmulas matemáticas denominadas funciones hash (y que se implementan como algoritmos hashing).

En resumen, no es más que un conjunto de caracteres alfanumérico de 128-256 bits, generado a partir de un texto plano. Suelen tener una longitud finita y se caracterizan por ser irreversibles y determinísticos.

- No involucran el uso de claves
- Determina una suma de verificación única (checksum) criptográfica sobre el mensaje

HASHING (Digest)



Algoritmos Hashing (Digest)

- MD5: Diseñado por Ronald Rivest con 128 bits (el mas usado).

  Ejemplo utilizando MD5
  Hash Resultante
  Hola: 4d186321c1a7f0f354b297e8914ab240
  Hola: -268801f78ba900ecb415989f7400b5c5

- SHA: Propuesto por la NSA a 160 bits

HASHING VS CIFRADO

Hashing – validar que el contenido no ha sido modificado sin necesidad de ver el contenido. (Integridad)

Cifrado – mantener en secreto el contenido para que pueda ser descifrado mediante una clave secreta. (Confidencialidad)

FIRMA DIGITAL

La firma digital consiste en la creación de un código, a través de la utilización de una llave privada, de modo que la persona o entidad que recibe un mensaje conteniendo este código pueda **verificar si el remitente es quien dice ser** e identificar cualquier mensaje que pueda haber sido modificado.

- La firma digital de un mensaje es un conjunto de datos que se añaden a dicho mensaje.
- Cada mensaje tiene una firma digital distinta.
- El mensaje puede ir cifrado o no, eso es opcional.
- La firma del mensaje se consigue cifrando con la clave privada el mensaje a enviar.
- Los algoritmos de clave asimétrica son lentos, así que para hacer más rápido el firmado digital de mensajes, se hace uso de las llamadas **funciones *hash***. Una función hash obtiene un ***resumen*** del mensaje original.

FIRMA DIGITAL

1. David redacta un mensaje
2. David firma digitalmente el mensaje con su **clave privada**
3. David envía el mensaje firmado digitalmente a Ana a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio
4. Ana recibe el mensaje firmado digitalmente y comprueba su autenticidad usando la **clave pública** de David
5. Ana ya puede leer el mensaje con total seguridad de que ha sido David el remitente

FIN