CESUR

UT4. Programación segura

PSP - DAM

Francisco Gallego Perona

Medios de comunicación

- Los medios de comunicación **distan mucho de ser ideales**.
- Los mensajes se pueden **deteriorar** o incluso **perder**.
- El medio es **compartido** con otros emisores y receptores.

Canal

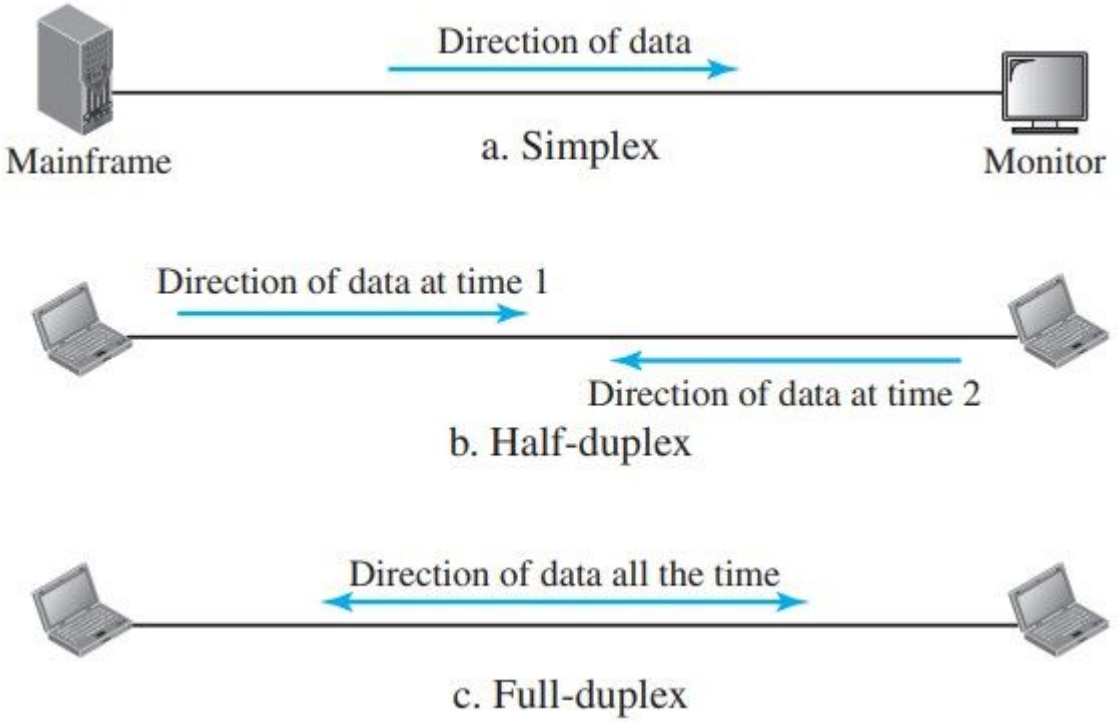
El canal suele ser bidireccional: permite la comunicación en ambos sentidos (emisor y receptor).

Duplex: ambas partes pueden actuar como emisor y como receptor.

- **Full-duplex**: Ambas partes pueden actuar de forma simultánea.
- **Half-duplex:** Ambas partes no pueden actuar de forma simultánea.

Simplex: Si un extremo actúa siempre como emisor y el otro como receptor pero no pueden actuar como el rol contrario.

Canal


Direction of data
Mainframe
a. Simplex
Monitor
Direction of data at time 1
Direction of data at time 2
b. Half-duplex
Direction of data all the time
c. Full-duplex

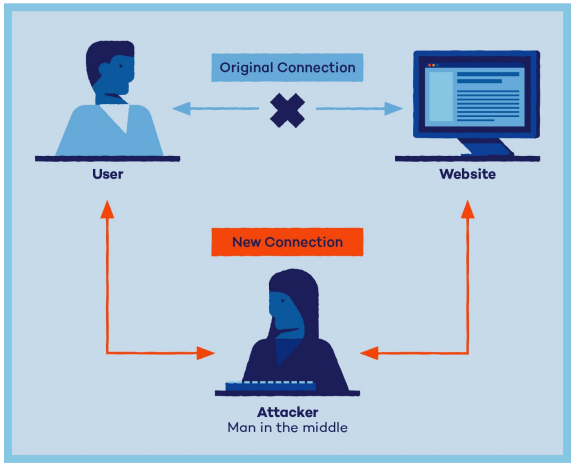
Aspectos de seguridad en las comunicaciones

Integridad

Los datos que recibe el receptor son idénticos a los enviados por el emisor. No se han alterado en ningún punto intermedio en el medio de comunicación.

Las alteraciones podrían ser por fallos en el medio o acción de alguien que busca alterar los datos.

- IP Spoofing
- ARP Spoofing
- DNS Spoofing



Aspectos de seguridad en las comunicaciones

Confidencialidad

Los datos transmitidos solo son inteligibles para el receptor previsto del mensaje.

Obtenemos confidencialidad de datos cuando encriptamos en el origen y desencriptamos en el destino. El único capaz de desencriptar el mensaje es el destino al que vamos a enviar el mensaje.

Aspectos de seguridad en las comunicaciones

Autenticación

El receptor del mensaje puede estar seguro de que el emisor del mensaje es quien espera que sea. El emisor es quien dice ser y no un suplantador.

Aspectos de seguridad en las comunicaciones

No repudio

El receptor del mensaje puede demostrar, una vez recibido un mensaje de un emisor, que el mensaje fue emitido por dicho emisor. De otra forma, si el emisor negara haber emitido dicho mensaje, le podrá refutar.

Funciones Hash

Hace corresponder a cada secuencia de bytes → una cadena de longitud fija y corta.

El cálculo hash para una secuencia de bytes es muy rápido.

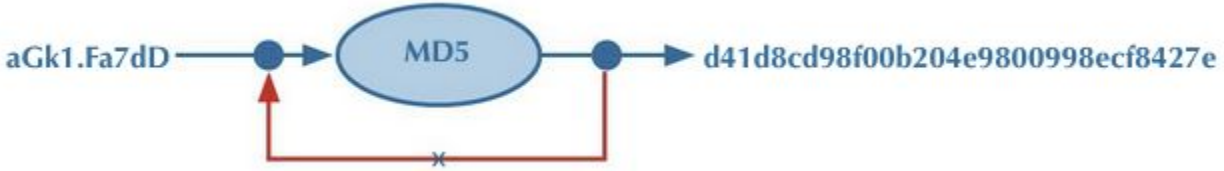
Algunas funciones hash son: MD5 y SHA-1

https://rosettacode.org/wiki/MD5/Implementation

Requisitos de funciones Hash

- **No reversibilidad**: Debe ser prácticamente imposible obtener una secuencia para la que la función de hash calcule un valor determinado. Debe haber un coste computacional enorme para encontrar la secuencia de bytes que dé lugar a un hash concreto.

  Colisión de hash: sucede cuando se busca y se encuentra el valor de hash mediante un ataque de fuerza bruta, por ejemplo.



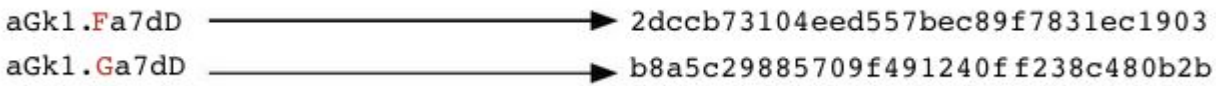
Requisitos de funciones Hash

- **Uniformidad**: El número de posibles secuencias es muy superior al número de posibles valores que puede tomar la función de hash. Cada posible valor de hash corresponderá a aproximadamente el mismo número de secuencias.

  Distribución uniforme de probabilidades de obtener los resultados de la función de hash.

Requisitos de funciones Hash

- **Discontinuidad**: Pequeñas variaciones en la secuencia de bytes deberían dar como resultado grandes variaciones en el valor del hash calculado. Si se cambia un sólo byte de un fichero de muchos mb, la variación de su hash debería ser enorme.



Criptografía

El objetivo de la criptografía es escribir mensajes de forma que sean ininteligibles excepto para el destinatario del mensaje.

Mensaje original → Mensaje cifrado/encriptado

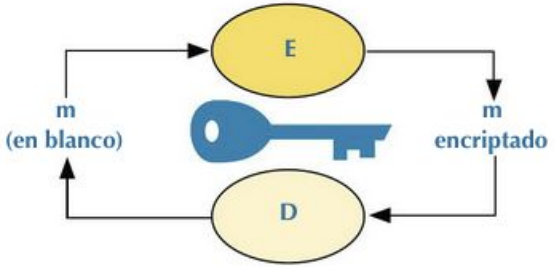
Un intento de descifrar un mensaje por parte de un emisor no previsto es un ataque criptográfico → Mediante fuerza bruta.

Criptografía simétrica (de clave privada)

Es la criptografía tradicional.

- Se utiliza la misma clave para **cifrar** y para **descifrar** un mensaje.
- Esta **clave es un secreto** entre emisor y receptor.

Se basa en una clave secreta... ¡Compartida!



Criptografía simétrica (de clave privada)

La criptografía de clave privada puede garantizar:

- **Confidencialidad**: Sólo emisor y receptor conocen la clave. Sólo el receptor puede desencriptar el mensaje.
- **Autenticación**: El receptor puede estar seguro de que sólo el emisor ha podido generar el mensaje.

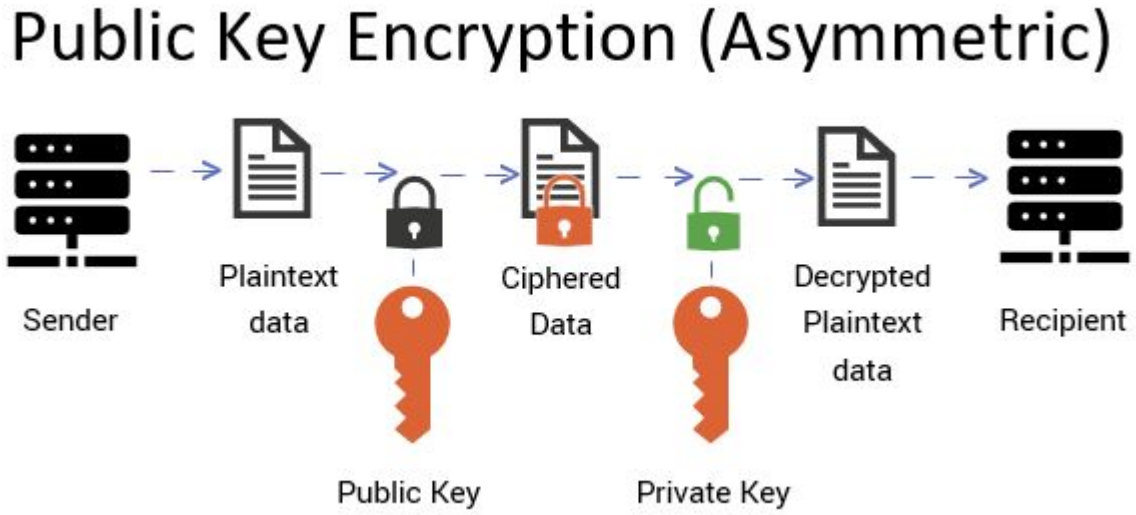
Criptografía de clave pública (asimétrica)

Permite el intercambio de información entre dos entidades sin compartir ningún secreto.

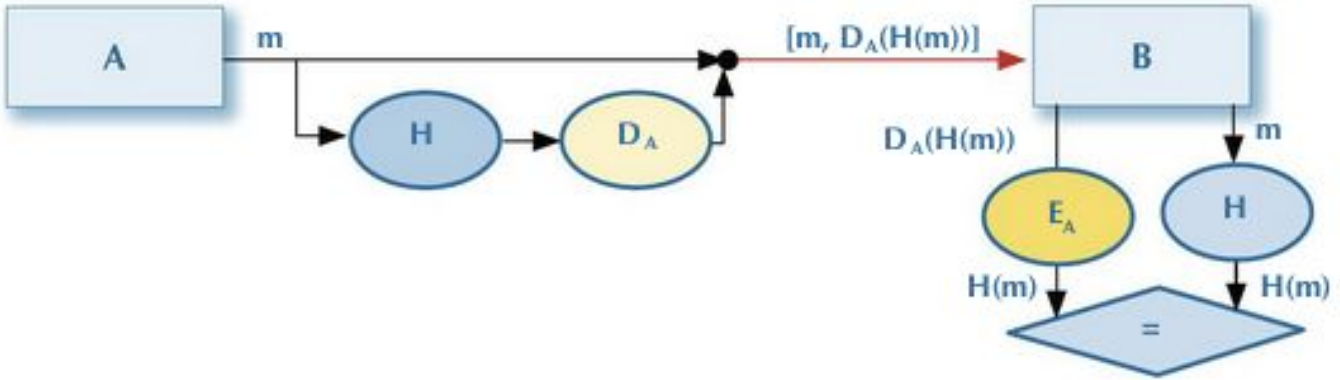
- Utiliza dos funciones matemáticas distintas para encriptación y desencriptación.
  - Para encriptación → clave pública
  - Para desencriptación → clave privada

Las funciones de encriptación (E) y desencriptación (D) son inversas la una de la otra.

Criptografía de clave pública (asimétrica)



Firma Digital



- Firma con clave privada
- Verificación con clave pública

Firma digital

¿Qué conseguimos con la firma digital?

- **Autenticación del emisor** del mensaje A por parte del receptor B.
- No repudio, porque **sólo A puede haber generado la firma digital D(H(m))**, dado que para calcular D hace falta la clave privada de A.
- **Verificación de la integridad del mensaje**. Porque B calcula el hash del mensaje H(m) y lo verifica con el calculado en origen por A, antes de enviarlo.

Criptografía con Java

Clase	Descripción
`MessageDigest`	Para funciones *hash* o *digest*.
`KeyGenerator`	Para generación y gestión de claves para criptografía simétrica.
`KeyPairGenerator`	Para generación y gestión de pares de claves para criptografía asimétrica o de clave pública.
`Cipher`	Para algoritmos de cifrado de datos.
`Signature`	Para algoritmos de firma digital.

Certificado digital

Documento que contiene información utilizada para criptografía de clave pública.

Permite acreditar la identidad de su poseedor o titular, que puede ser una persona o una entidad.

Certificado digital = DNI

Contiene (entre otros elementos):

- nombre del titular
- clave pública

Certificado digital

Un certificado está **firmado digitalmente**. Contiene una firma digital de sus contenidos.

- Garantizamos la **integridad** del certificado. Detectamos si se hace cualquier cambio en él posteriormente a su creación y firma.
- Identificamos al **creador** del certificado digital. Cualquiera puede crear un certificado digital con la información que quiera; lo único que puede garantizar la corrección de los datos contenidos en un certificado y que pertenecen a la persona o entidad es que esté firmado por un emisor de confianza.

Certificado digital

Estructura del certificado X.509

Version		Identificador de la versión.	Versión 1	Versión 2	Versión 3
Serial Number		Número de serie. Cada certificado digital emitido por una entidad certificadora debe tener un número de serie distinto.			
Signature Algorithm ID		Identificador del algoritmo utilizado para generar la firma digital del certificado.			
Issuer Name		Nombre del emisor, es decir, de la entidad que ha creado el certificado.			
Validity period	Not before	Periodo de validez del certificado, delimitado por la fecha inicial (*not before*) y la fecha final (*not after*).			
	Not after				
Subject name		Nombre de la persona o entidad a la que se identifica en el certificado, es decir, del titular.			
Subject Public Key Info	Public Key Algorithm	Información de clave pública. Incluye la identificación del algoritmo para el que está creada la clave (los distintos algoritmos utilizan distintos tipos de claves públicas), y la clave pública en sí.			
	Subject Public Key				
Issuer Unique Identifier		Identificador numérico correspondiente al campo anterior "Issuer Name". Si está presente, lo sustituye como identificador del emisor del certificado (*issuer*).			
Subject Unique Identifier		Identificador numérico correspondiente al campo anterior "Subject Name". Si está presente, lo sustituye como identificador del titular del certificado (*subject*).			
Extensions		Extensiones. Se explican a continuación.			
Certificate Signature Algorithm		Identificación del algoritmo de firma digital empleado para generar la firma digital de todos los contenidos previos, y firma digital realizada con este algoritmo utilizando la clave privada del emisor (*issuer*) del certificado.			
Certificate Signature					

Certificado digital

¿Quién se considera un emisor de confianza de certificados digitales?

Una **Autoridad Certificadora** (CA - Certification authority) → Es una entidad facultada legalmente para emitir certificados digitales.

En España → FNMT (Fábrica Nacional de Moneda y Timbre)

Para validar la firma de un certificado digital emitido por una CA se necesita la clave pública de esa CA.