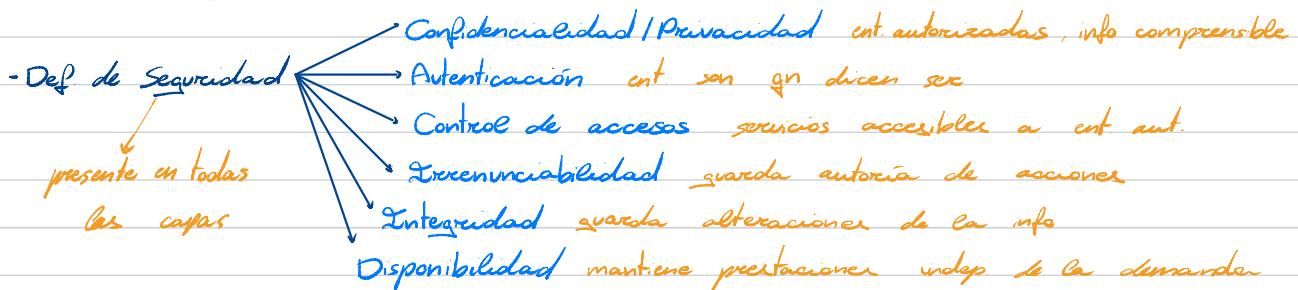


Tema 4: Seguridad en Redes• Introducción

Red segura  $\Rightarrow$  Se garantizan todos los aspectos

No hay red segura al 100 %



- Ataque de seguridad  $\rightarrow$  Tipos

- $\rightarrow$  Sniffing escuchar
- $\rightarrow$  Spoofing suplantación
- $\rightarrow$  Man-in-the-middle interceptación
- $\rightarrow$  Distributed Denial-of-Service
- $\rightarrow$  Malware

• Cifrado

$$\text{Texto llano/claro } P \xrightarrow[E_k(C)]{} \text{Texto cifrado } C$$

Dif. Encontrar clave de cifrado  $K$  y de descifrado  $K'$

- Cifrado simétrico  $K \cdot K'$

- $\rightarrow$  DES Data Encryption Standard, esquema de sustitución monoalfabético
  - $\hookrightarrow$  Se encadenan DES Doble / 3DES
- $\rightarrow$  3DEA International Data Encryption Algorithm

- Cifrado asimétricos

Usamos CA) 2 claves:  $K_{\text{pub}} \neq K_{\text{priv}}$

Claves para cifrar  $\neq$  para descifrar

Cifrar  $\rightarrow C = E_{K_{\text{pub}}} (P)$  / Descifrar  $P = D_{K_{\text{priv}}} (C)$

$\hookrightarrow$  enviamos  $C = E_{K_{\text{priv}}} (P) \Rightarrow$  Autenticación

$\rightarrow$  RSA (Rivest Shamir y Adleman)

1- Elige  $p$  y  $q$  primos grandes

2-  $n = p \cdot q \wedge z = (p-1)(q-1)$

3- Elige  $d$  primo respecto a  $z$

4- Calcular  $e \leftarrow ced^{-1} \pmod{z}$

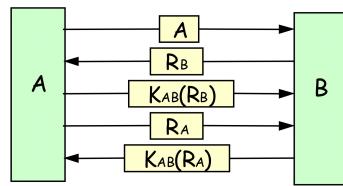
5-  $K_{\text{pub}} = (e, n) \wedge K_{\text{priv}} = (d, n)$

$$C = P^e \pmod{n}$$

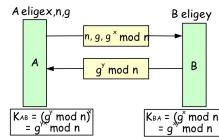
$$P = C^d \pmod{n}$$

## • Autenticación

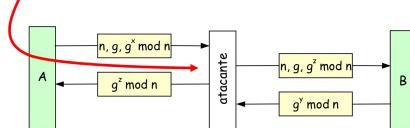
→ Esquema recto - respuesta



→ Intercambio de Diffie-Hellman



- Ataque: man-in-the-middle



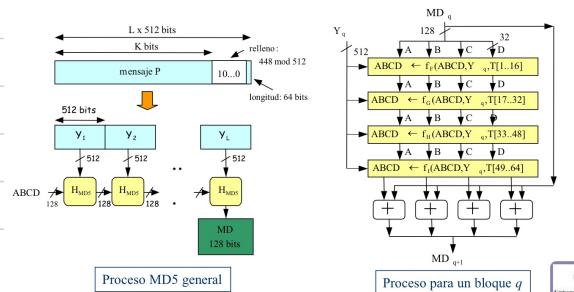
## • Funciones Hash (Compendios)

- Irreversibles de cálculo sencillo
- M = texto de entrada, long variable
- M → HCM (con long fija de 256 o 512 bits)
- HCM → M
- Dado M, imposible encontrar M' tg M ≠ M' ∧ HCM(M) = HCM(M')

→ Message Digest 5 (MD5)

MD5 ("Message Digest 5", RFC 1321):

- Proceso (resumen de 128 bits):
  - Relleno 100..0 de longitud máxima 448 bits
  - Adición de campo de longitud de 64 bits
  - División del mensaje en bloques de 512 bits
  - Procesamiento secuencial por bloques

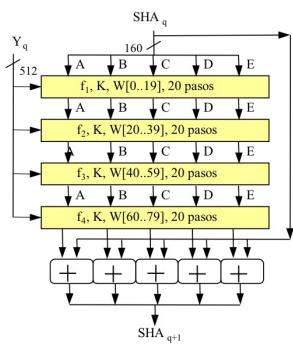
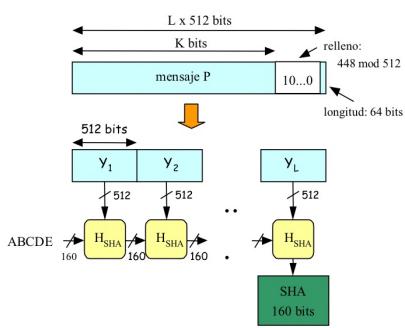


→ Secure Hash Algorithm 1 (SHA-1)

SHA-1 ("Secure Hash Algorithm 1", NIST 1993):

### ○ Proceso (resumen de 160 bits):

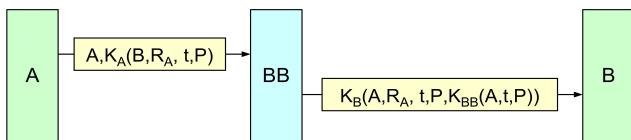
- Relleno 100..0 de longitud máxima 448 bits
- Adición de campo de longitud de 64 bits
- División del mensaje en bloques de 512 bits
- Procesamiento secuencial por bloques



## • Firma digital

- Receptor puede autenticar al emisor
- No haya repudio
- Emisor tiene garantías de no falsificación

Firma con clave secreta. Big Brother



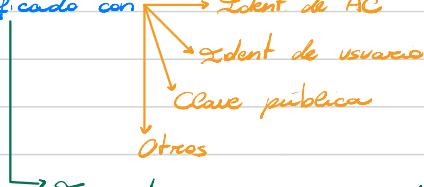
Firma digital con clave asimétrica Doble cifrado

- Uno privacidad, otro autenticación
- Para firmar: enviar  $K_{pubB} \circ K_{privA}(r)$
- Receptor:  $K_{pubA} \circ K_{privB} \circ K_{pubB} \circ K_{privA}(r) = r$
- Hay que asegurar la asociación de la ident A con su clave



Certificados digitales  $\Rightarrow$  emitidos por Autoridades de Certificación (AC)

- 1- Usuario obtiene sus claves priv y pub
- 2- Envía solicitud firmada a AC con su ident y su clave pub
- 3- AC comprueba y emite el certificado con



→ Firmado con clave priv de AC para no falsif

→ Formato: X.509  $\rightarrow$  Campos:

Field	Explanation
Version	Version number of X.509
Serial number	The unique identifier used by the CA
Signature	The certificate signature
Issuer	The name of the CA defined by X.509
Validity period	Start and end period that certificate is valid
Subject name	The entity whose public key is being certified
Public key	The subject public key and the algorithms that use it

## • Resumen Seguridad

- Confidencialidad → Cifrado
- Autenticación → Peto-Respuesta / Firma digital
- No repudio → Firma digital
- Integridad → Comprobadas (Func. Hash)
- Disponibilidad → Otras cosas tb necesarias