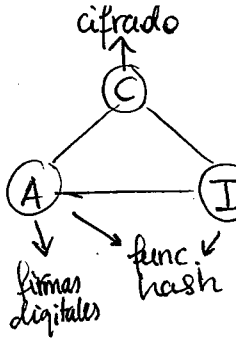
RESUMEN SEGURIDAD REDES

SEG. EN REDES = DISPONIBILIDAD + SEG. INFORMACIÓN

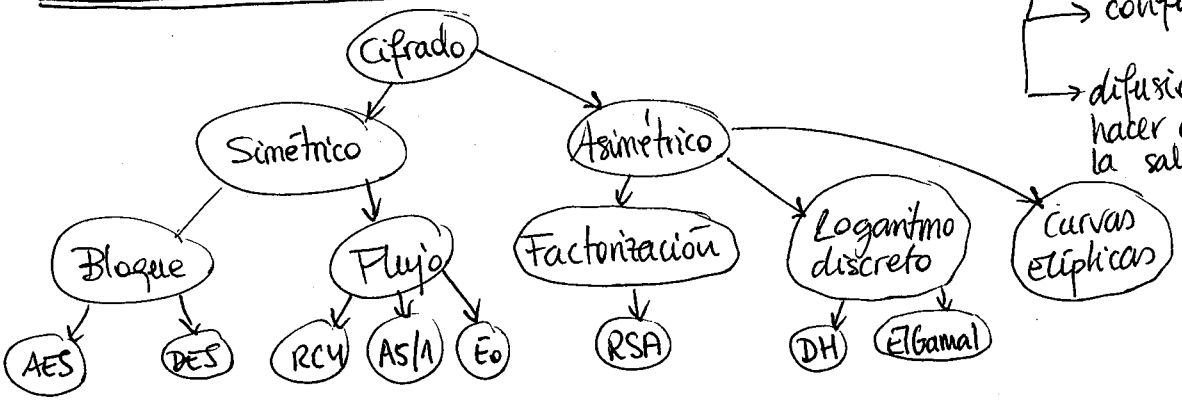
≈ CIA ≡ Confidencialidad
Integridad
Autenticación



CRIPTOLOGÍA = CRIPTOGRAFÍA + CRIPTOANÁLISIS

CRIPTOGRAFÍA CLÁSICA (SUSTITUCIÓN) → cifrado César
→ monoalfabético
→ polialfabético

CRIPTOGRAFÍA MODERNA



Mecanismos básicos
→ confusión: ocultar relac texto plano, texto cifrad
→ difusión: hacer depender la salida de y clave la entrada lo máximo posible

CIFRADO SIMÉTRICO

- POR BLOQUE

- ECB (Electronic CodeBook): mensaje troceado en bloques que se encriptan de forma separada. Códigos iguales generan resultados igu

$C_i = K_E(P_i)$ $\quad P_i = K_D(C_i)$

- CBC (Cipher Block Chaining): cada bloque hace un XOR con el bloque previo ya cifrado. Depende de un vector de inicialización.

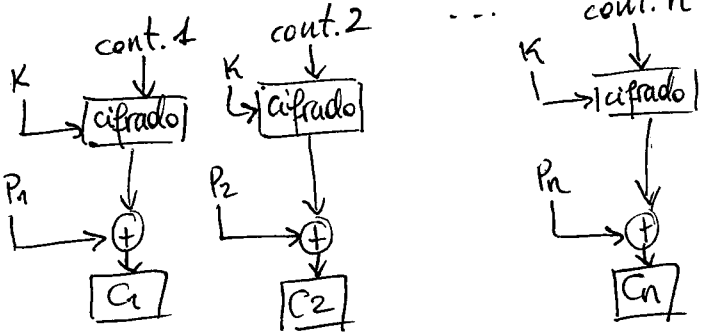
$C_i = K_E(P_i \oplus C_{i-1})$ $\quad P_i = K_D(C_i) \oplus C_{i-1}$ $\quad C_0 = VI$

- PCBC (Propagating Cipher Block Chaining): diseñado para provecar un mayo cambio en la salida con un pequeño cambio en la entrada.

$C_i = K_E(P_i \oplus P_{i-1} \oplus C_{i-1})$ $\quad P_0 = VI$ $\quad C_0 = 0$

$P_i = K_D(P_i) \oplus P_{i-1} \oplus C_{i-1}$ $\quad P_0 = VI$ $\quad C_0 = 0$

- CTR (Counter mode): convierte el cifrador de bloques en uno de flujo



- DE FLUJO:

Combina cada bit del flujo de clave con el texto legible y obtiene el texto cifrado

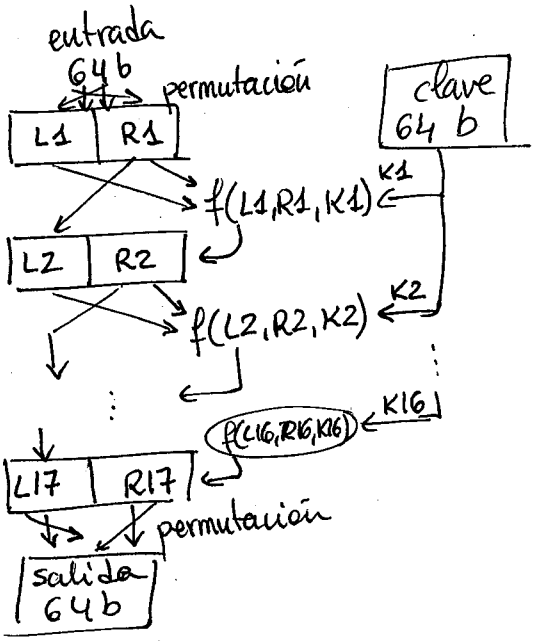
$c_i = Ks_i \oplus m_i$ $\quad m_i = Ks_i \oplus c_i$

m_i = i-ésimo bit mensaje plano
Ks_i = i-ésimo bit clave
c_i = i-ésimo bit cifrado

DES: DATA ENCRYPTION STANDARD

clave de 56 bits + 8 de paridad
bloques de texto plano de 64b
rotísimo (por fuerza bruta menos 1 día)

permutación inicial
16 ciclos con clave distinta
permutación final



3DES: básicamente cifrar, descifrar y cifrar con DES con claves diferentes

AES: ADVANCED ENCRYPTION STANDARD

bloques de 128 b
claves de 128, 192 o 256 b
No es de tipo Feistel, sin que usa álgebra de cuerpos finitos, cuerpo de Galois, $GF(2^8)$
Aunque sí usa cajas S

CIFRADO ASIMÉTRICO

El algoritmo más conocido y utilizado es RSA:

1. Elegir dos primos grandes p y q
2. Calcular $n = pq$ y $z = \varphi(n) = (p-1)(q-1)$
3. Elegir e menor que n tal que e y $z = \varphi(n)$ sean coprimos. $mcd(e, \varphi(n)) = 1$
4. Elegir d inverso multiplicativo con e $\mod \varphi(n) = \mod z$, e.d., $ed \equiv 1 \pmod z$.

clave publica: $\{n, e\}$ clave privada $\{n, d\}$

$c = m^e \pmod n$ $m = c^d \pmod n$

INTEGRIDAD DE LOS MENSAJES

FUNCIONES HASH

Funciones que dado mensaje m calcula una salida de tamaño fijo.
Es prácticamente imposible encontrar colisiones y es irreversible
Más conocidas: MD-5 → salida de 128b en un proceso de 4 pasos
SHA-1 → salida de 160b

CÓDIGO AUTENTIFICACIÓN MENSAJE → MAC

$m :=$ mensaje
$s :=$ secreto compartido

Alicia calcula $h = H(m+s)$ y envia a Bob (m,h)
Bob recibe (m,h), conoce s, calcula $h' = H(m+s)$ y comprueba que $h = h'$.

El estándar más popular hoy en día es HMAC (utiliza MD5 ó SHA-1)

FIRMAS DIGITALES

Se cifra el mensaje con la clave privada del emisor. Cualquiera puede comprobar la firma $K_E-(m)$ con $K_E+(K_E-(m)) = m$.
Computacionalmente es muy caro, así que se firman resúmenes del mensaje o el hash del mensaje.

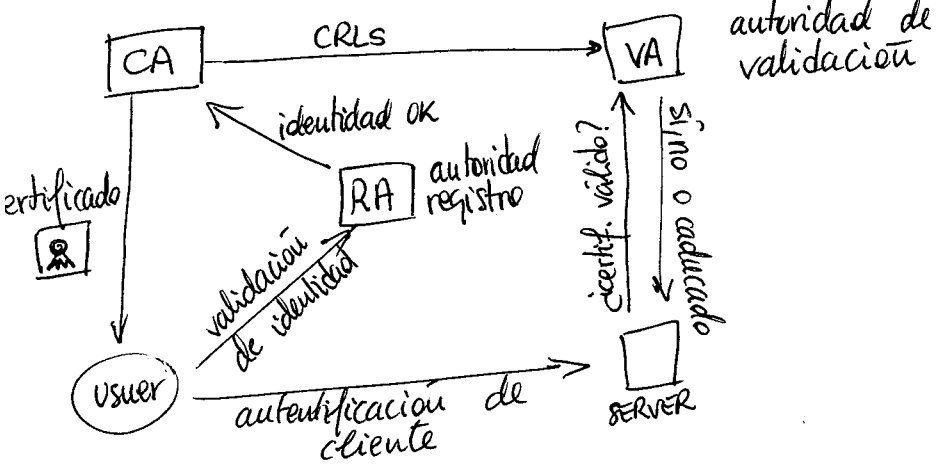
Posible origen esquema híbrido

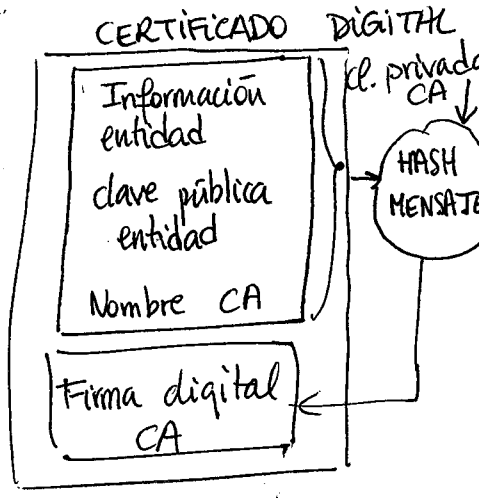
CERTIFACIÓN CLAVE PÚBLICA

- AUTORIDAD CERTIFICADORA (CA)

Asocian claves públicas con entidades

Pubic Key Infraestructure





Más conocidos: X.509

AUTENTICACIÓN DE EXTREMO

Esquema híbrido une CIA completamente
+ autentificación con CAs.
+ ↓ este tema

ALGO QUE SABEMOS
- contraseñas
- pin
- claves criptográficas

ALGO QUE TENEMOS
- DNIs
- tarjetas de coord.
- Tokens OTPs
- teléfonos

ALGO QUE SOMOS
- firma manuscrita
- huella dactilar
- Retina
- Voz

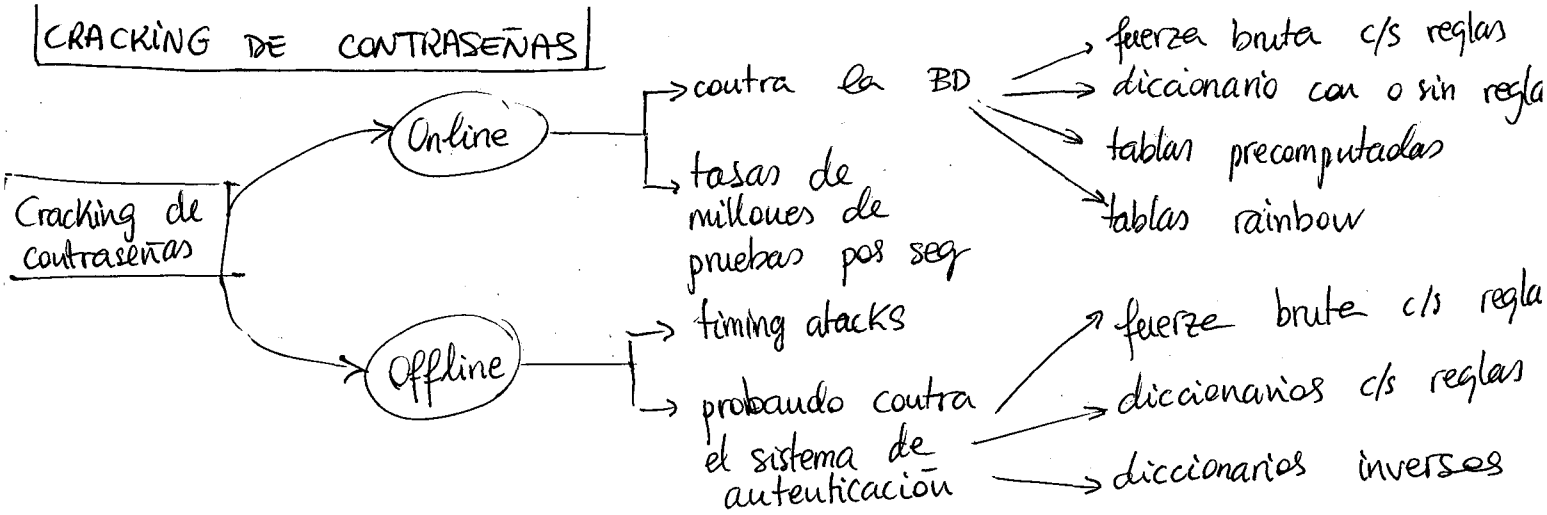
CONTRASEÑAS

PAO, passphrases, patrones de teclado, gestores de contraseñas

ATAQUES A CONTRASEÑAS

- Al servidor
  - al SO
    - buffer overflow
    - head overflow
    - errores de configuración
  - a los servicios/apps
    - inyección SQL, LDAP, comandos
    - XSS
    - ataques a las APIs
- A la red: ataques contra la comunicación cliente-servidor
  - confidencialidad: obtener token mientras viaja por la red: SNIFFING
  - integridad: modificación de la comunicación C-S: ARP spoofing, MITM
  - autenticación: suplantaciones de identidad: HIJACKING, SPOOFING
- Al cliente
  - Ing. social: manipulación de personas: ataques de phishing, ataque de CE
  - (Digital) Trashing: búsqueda de información útil (post-it, linked-in)
  - Shoulder Surfing

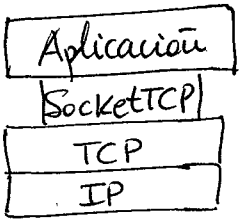
CRACKING DE CONTRASEÑAS



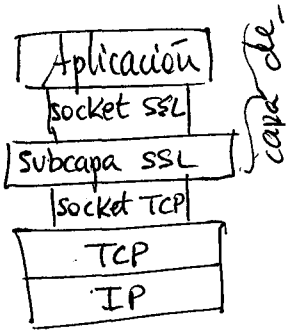
Observación: ALMACENAMIENTO SEGURO DE CONTRASEÑAS EN BD

SEGURIDAD EN LAS ARQUITECTURAS DE RED

SSL ó TLS con TCP/IP



API TCP



- Herramientas de cifrado
  - alg. clave pública → RSA
  - alg. clave simétrica → DES, 3DES; RC2 (bloques), RC4 (flujo)
  - alg. MAC (Msg Authetication Code)
- Negociación (Handshaking) del sistema de transferencia
  - Autenticar servidor
  - acordar alg. cifrado
  - establecer claves
  - autenticar cliente (opcional)

Procedimiento handshaking:

1. El cliente envía lista de algoritmos que soporta + nº de replica cliente (Rc
2. Servidor elige algoritmo de la lista.
3. El servidor envía elección, certificado y nº de replicación servidor (R
4. Cliente verifica certificado, extrae clave pública servidor, genera el "pre-master secret", lo encripta con la cl. públ. serv. y se la envía
5. El cliente y el servidor calculan independientemente las claves de encriptación y MAC a partir del "pre-master secret" y los nºs de unicidad (ambos comparten estas 4 claves).
6. El cliente envía un MAC de todos los mensajes del handshak
7. El servidor envía un MAC de todos los mensajes del handshak

→ protegen al handshake de ser observados (evitan suplantaciones de identidad)

* Mirar generación de claves diapositivas Eloy.

1.

1) $pq = 21 = n$ $\quad \varphi(n) = 12$

$\text{mcd}(5, 12) = 1$ ✓

2) $d = 5$ porque $n.d \pmod{\varphi(n)} = 1$

3) clave pública → $\{e = 5,\ n = 21\}$ clave privada → $\{d = 5,\ n = 21\}$

4) $M = 9 \longrightarrow C = M^e \bmod(n) \Rightarrow C = 9^5 \pmod{21} \Rightarrow$

$\Rightarrow C = 18$

2. ~~B)~~ C)

3. B)

4. A)

5. D)

6. ? (a saltao

7. C)

8. d)

9. Igual que 1)

10. C)

POLÍTICAS DE CONTRASEÑAS

$32 + 10 + 26 + 26 = 94$

- POL 1

$94^6 + 94^7 + 94^8 = 6'16 \cdot 10^{15}$

$t_1 = 781$ años

- POL 2

~~$52^6 + 52^7 + 52^8 = 5'45 \cdot 10^{13}$~~

~~$6'16 \cdot 10^{15} - 5'45 \cdot 10^{13} = 6'1 \cdot 10^{15}$~~

~~$t_1 = 781$ años~~

~~$t_2 = 771,3$ años~~

principio de inclusión-exclusión

TEMA 2 | SEGURIDAD Y CRIPTOGRAFÍA

SEGURIDAD DE LA INFORMACIÓN

C.I.A. ≡ Confidencialidad, Integridad, Autentificación

Confidencialidad ≈ Secreto
Integridad ≈ Modificación
Autentificación ≈ Identidad

- CONFIDENCIALIDAD: El receptor y no otro puede "entender" el contenido
  - El emisor cifra el mensaje
  - El receptor descifra el mensaje
- AUTENTIFICACIÓN: El receptor quiere confirmar la identidad del emisor
- INTEGRIDAD: El receptor quiere asegurarse que el mensaje no ha sido alterado sin detectarlo.
- DISPONIBILIDAD: Los servicios deben ser accesibles y estar disponibles para los usuarios.

¿Qué hacen los enemigos?

- → espiar mensajes ajenos
- → insertar activamente mensajes en la conexión
- → suplantación de identidad fingiendo la dirección fuente del paquete
- → secuestro de la conexión en curso poniéndose en el lugar del emisor, receptor o ambos.
- → provocar una denegación de servicio.

PRINCIPIOS DE LA CRIPTOGRAFÍA