

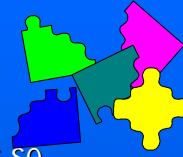
Seguridad en la Red
Certificados,
Autoridades Certificantes
SSL-S/MIME



Alejandro Román - Marcelo Utard
Fac. de Ingeniería
Universidad de Buenos Aires

1

Elementos



Las aplicaciones criptográficas más usuales se construyen con estos 3 elementos:

- **Funciones de hash seguras**

(Secure Hash Functions)

- **Cifradores** *(Ciphers)*

- Simétricos, convencionales o de secreto compartido *(symmetric ciphers)*
- Asimétricos o de clave pública *(public key cyphers)*

Hash Function

- $::$ = una función H que toma un string M , y produce otro, h , de tamaño fijo (generalmente mas corto)
- Al resultado (h) de aplicar una *hash function* a un string se lo suele llamar simplemente *hash* del string M

Secure Hash Functions

- $h = H(M)$ con los siguientes requisitos:
 - Dado M es fácil computar h
 - Dado h es difícil encontrar el M original
 - Dado M , es difícil encontrar otro M' tal que $H(M) = H(M')$
- 2 tipos de s.h.f.:
 - Sin clave
 - Con clave (ej. usar una s.h.f sin clave y encriptarla). Para MACs
- Aplicaciones: integridad de mensajes o archivos, firma de digestos en vez de mensajes.

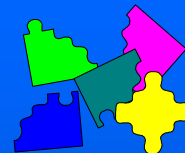
Secure Hash Functions

- también llamadas:
 - compression function,
 - contraction function,
 - message digest,
 - fingerprint,
 - cryptographic checksum,
 - data integrity check (DIC),
 - manipulation detection code (MDC),
 - message authentication code (MAC),
 - data authentication code (DAC)

"Secure" hashes

- SNEFRU (128/256 bits); El SNEFRU de 2 pasos se puede quebrar, usando una PC, en 3 minutos [birthday: dado M, hallar M' cuyo $H(M')=H(M)$], o en 1 hora (hallar un mensaje M dado un hash h)
- N-HASH
- MD2 (Message Digest-2, Ron Rivest, 128 bits, mas lento, menos seguro que MD4, usado en PEM)
- MD4 (Message Digest-4, Ron Rivest, 128 bits, muy usado)
- MD5 (Message Digest-5, Ron Rivest, 128 bits, MD4 con mejoras, muy usado, usado en PEM, SSL)
- SHA (secure hash algorithm, 160 bits, usado en DSS, SSL)
- Otros

Elementos

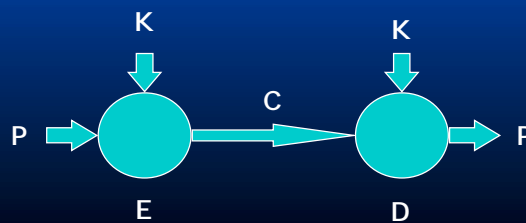


Las aplicaciones criptográficas más usuales se construyen con estos 3 elementos:

- Funciones de hash seguras (*Secure Hash Functions*)
- Cifradores (*Ciphers*)
 - Simétricos, convencionales o de secreto compartido (*symmetric ciphers*)
 - Asimétricos o de clave pública (*public key cyphers*)

Criptografía Simétrica (o de secreto compartido)

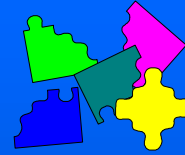
- $C = E_k [P]$ (cifrar)
- $P = D_k [C]$ (descifrar)
- La clave (K) es la misma para ambas operaciones



Algoritmos simétricos

- **DES** (block, clave de 56 bits)
- **RC2** (block, Ron Rivest, reemplazo para DES, clave de tamaño variable)
- **RC4** (stream, Ron Rivest)
- **IDEA** (block, international data encryption std. clave de 128 bits)

Elementos

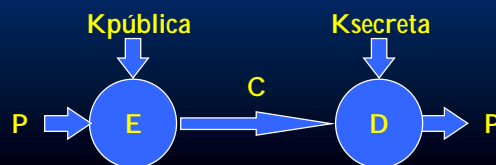
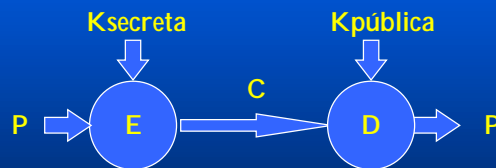


Las aplicaciones criptográficas más usuales se construyen con estos 3 elementos:

- Funciones de hash seguras (*Secure Hash Functions*)
- Cifradores (*Ciphers*)
 - Simétricos, convencionales o de secreto compartido (*symmetric ciphers*)
 - **Asimétricos o de clave pública** (*public key cyphers*)

Criptografía Asimétrica (Sistemas de Clave Pública)

- Mediante un programa, el usuario genera un PAR de claves. Una es la pública, la otra es la privada.
- Si se encripta con una, se desencripta con la otra.



Criptografía de clave pública

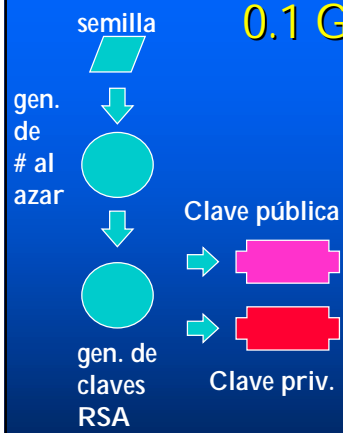
- Deducir una clave a partir de la otra es computacionalmente irrealizable
- 100-1000 veces más lentos que los simétricos
- claves mucho más largas que los simétricos
- Solución para el problema de distribución de claves, pero no completa:
 - **Ataque: sustitución de clave pública**

Algoritmos de clave pública

- Diffie-Hellman (distribución de claves)
- RSA (distribución de claves, encriptado)
- ElGamal (distribución de claves, encriptado)
- DSA (firmas digitales)
- La mayor parte basados en uno de estos tres problemas difíciles:
 - logaritmo discreto:
 - p, primo: g y M enteros,
 - encontrar x tal que $g^x = M \pmod{p}$
 - factorización
 - knapsack (dado un conjunto de números particulares, encontrar un subconjunto cuya suma sea N)

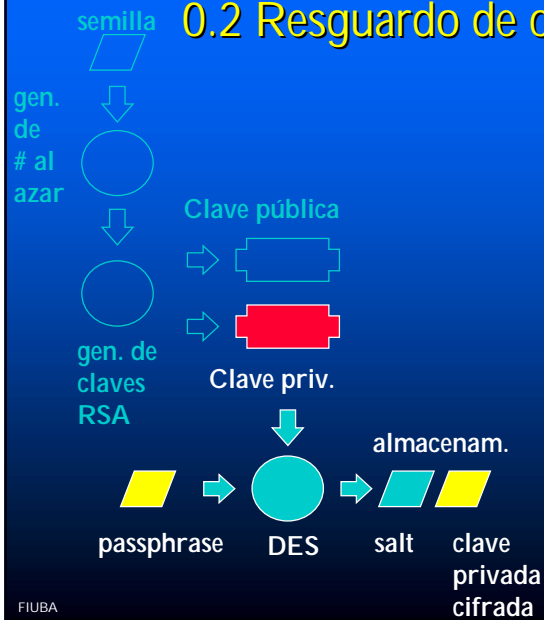
2

Caso práctico 0.1 Generación de claves



Caso práctico

0.2 Resguardo de clave privada



FIUBA

17

Clave privada del solicitante

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4, ENCRYPTED

DEK-Info: DES-EDE3-CBC, 93832DFCC1628BCB

K2uyyzgaN0Czcebwhd7jpp0lRPa89Yu03MwZlRPjLUQBxjnQC0jVgX7U00NwE+Tf
nHTGW78Go/h081z4d2k/NitW+szLJctH/HsqGCL7UeeKCrfezz2+X/JbDznw0I/W
+WPhiw45JNAx0t/c5D3R+EukJdQ2LsiCMXsPCFbS7fZdSM/dNtw5GsGhrVRsheh/
T2polwdKy1VIYJht7N2+PylersLjdb75m4XT3xuc8pgmENryBFEK8nFRptp56EfT
8AG1RzzKi/7rydq6T7c9ZJfCeDCu04WF8N+A3BuWriQn07mYoIgaBNMbqfPyJff
BAiQXVf1CUMYYNHuLHO11VfbnfTpuCPI7RU62/jw8wERrbmmZul2t5jgdUYtYUp9
WGQ1+Vd21KmzLJQSWXNrJW1VUs05vezNM/osPUpOCRdzjtjSKkHwjJr9bK8CbKUj
RP7o3jHgMkjDC9MdbfkwcgTi3mMwzKQa4b3L8A4CS3t4sdsvzz4NYXx1KuyN+JG
f8dfilUpGseS/YNwGZyxftVoVqzikNrt5n5ajfK0uVMPm1nIjIQkLABmTxVOGWP
74XccrK3m3dujucM5HkCBRBJJpc2tHfkqLTS2iQF+gW8ofVmIodqYgOga420mKGm
montBaBaQ3Wzgj7t4ppaCAMRD75TJPWahxfff0o49YR6NQ70i7LmENkxBDRR7kxk
o4cmtyT0AQHXk8BKGNrWclwWms1y9MQO1PH9m0yD0iEV2ETog+Snlbjcz5f+Oyh
BbBiIGYetz57bX8EOw0WWWJbjlJcJLkzTPswsSGWulaW/OKXc0tJfQ==

-----END RSA PRIVATE KEY-----

FIUBA

18

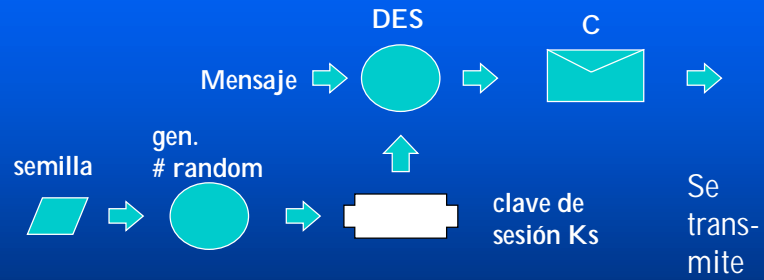
2. Aplicaciones

- Privacidad mediante criptografía simétrica y asimétrica
- Firma mediante criptografía asimétrica
- Certificados: Distribución segura de claves públicas
- Autenticación y control de acceso mediante criptografía asimétrica y certificados

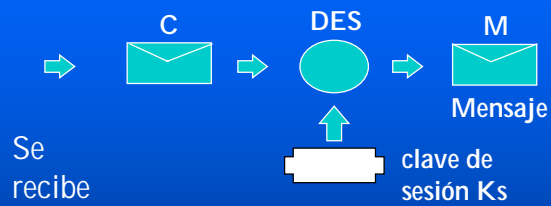
Transferencias Privadas mediante cripto asimétrica

- Para enviar un mensaje a X, se obtiene primero la clave pública de X, y se cifra el mensaje con ésta.
$$C = E_{k_x} [P]$$
- El destinatario descifra el mensaje usando su propia clave privada.
$$P = D_{k_x'} [C]$$
- Obsérvese que se utilizó el par de claves del destinatario.
- Obsérvese que no hay autenticación del remitente

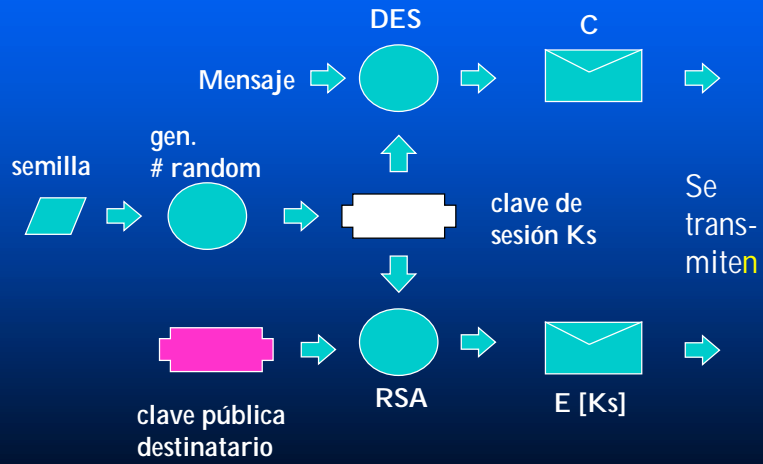
Privacidad, caso práctico - 1. Cifrado



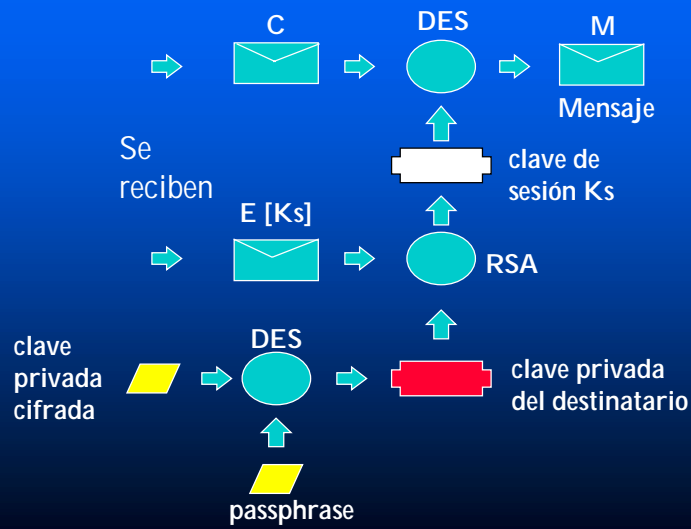
Privacidad, caso práctico- 2. Descifrado



Privacidad, caso práctico - 1. Cifrado



Privacidad, caso práctico- 2. Descifrado



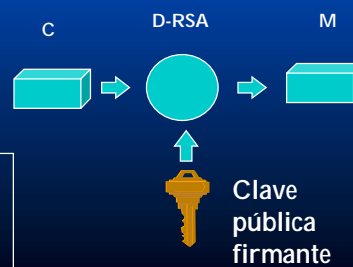
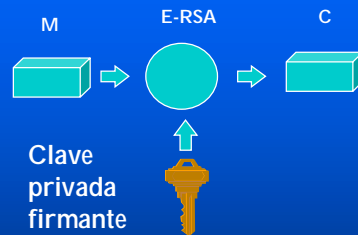
2. Aplicaciones

- Privacidad mediante criptografía simétrica y asimétrica
- **Firma mediante criptografía asimétrica**
- Certificados: Distribución segura de claves públicas
- Autenticación y control de acceso mediante criptografía asimétrica y certificados

Firmas digitales (*digital signatures*)

- Se usa un sist de clave pública, p.ej. el RSA
- Para firmar un mensaje, el remitente lo encripta usando su propia clave privada.
- Para autenticar el mensaje, el destinatario lo descifra usando la clave pública del remitente.
- Obsérvese que se utiliza el juego de claves del remitente

Firma digital mediante cripto asimétrica



Si - Autent. remitente
No - Privacidad

Firmas Digitales

- Si para firmar encriptáramos todo el mensaje, la firma sería del tamaño del mensaje
- Se obtiene un hash del mensaje, llamado *fingerprint*, y se firma el fingerprint
- El mensaje puede ir en claro (sin encriptar)

Firma Digital, caso práctico

1 - Operación de Firma

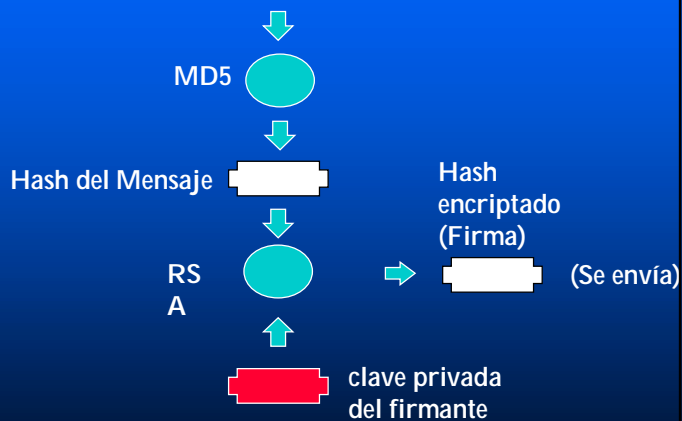
Mensaje M  → (Se envía)



Firma Digital, caso práctico

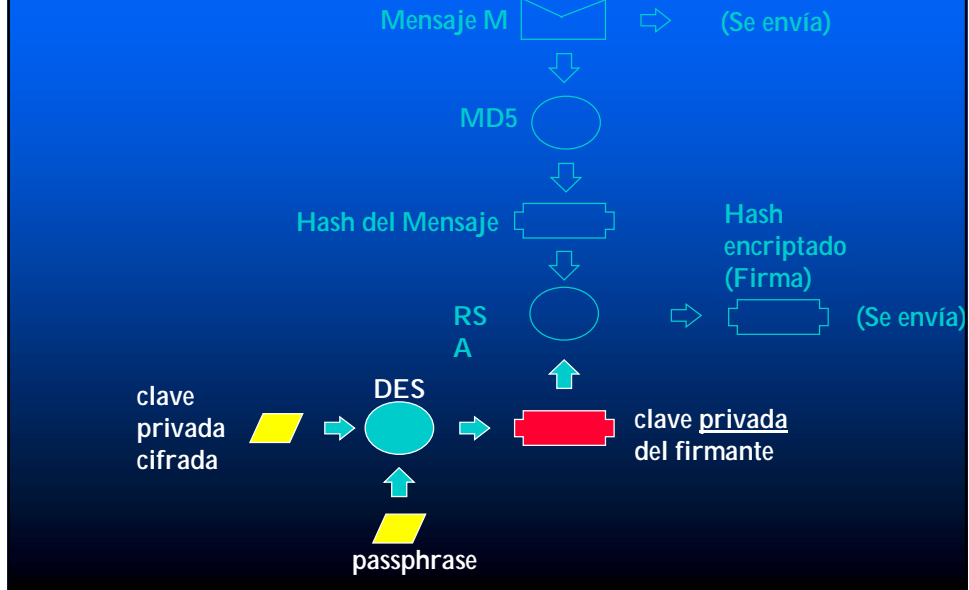
1.1 Firma de Hash en vez del mensaje

Mensaje M  → (Se envía)



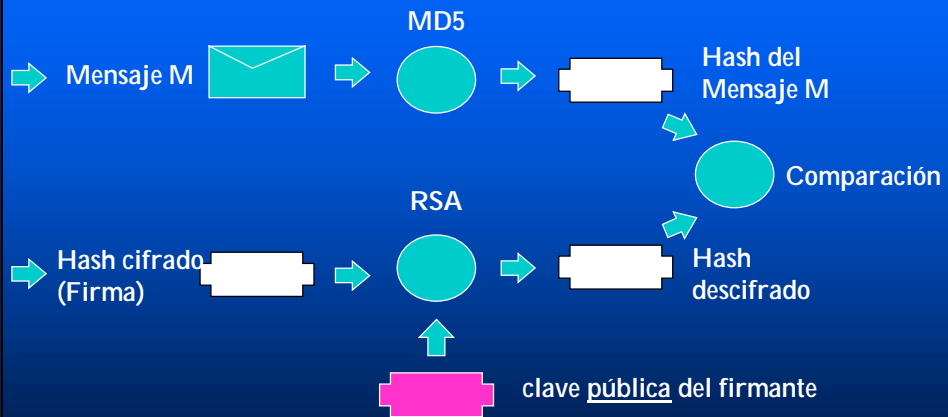
Firma Digital, caso práctico

1.2 Recuperación de la clave privada



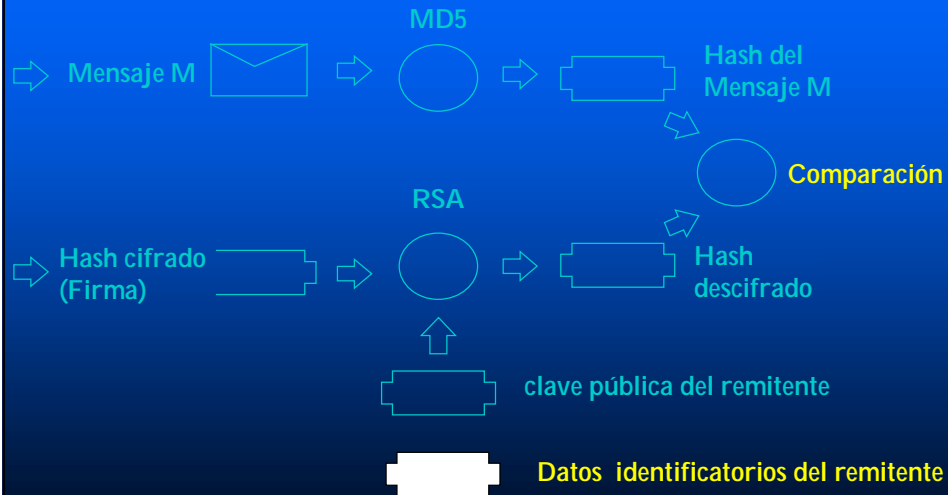
Firma, caso práctico

2.0 Verificación de Firma



Firma, caso práctico

2.1 Información final al usuario



Sistemas combinados

- Las técnicas se pueden combinar: Si el mensaje + fingerprint + firma se cifra a su vez con la clave pública del destinatario, se obtiene un mensaje a la vez privado y autenticado.
- El remitente debe obtener en forma segura la clave pública del destinatario, de no ser así se compromete la privacidad del intercambio
- El destinatario debe obtener en forma segura la clave pública del remitente, de no ser así se compromete la autenticidad del mensaje

2. Aplicaciones

- Privacidad mediante criptografía simétrica y asimétrica
- Firma mediante criptografía asimétrica
- **Certificados:**
Distribución segura de claves públicas
- Autenticación y control de acceso mediante criptografía asimétrica y certificados

Certificados de clave pública

- Objeto: acreditar una relación entre una identidad (y/o sus atributos) y una clave pública.
- Un **certificado** de clave pública es una estructura de datos que contiene
 - el nombre de un usuario (el "*subject*"),
 - su clave pública,
 - el nombre de una entidad (el "*issuer*", A.C.) que garantiza que la clave pública está asociada al nombre.
- Estos datos son firmados criptográficamente usando la clave privada del "*issuer*" (A.C.)

Identidad: Nombres distinguibles (*distinguished names*)

- Rec. ITU-T serie X.500
 - X.500, X.501, X.509, X.511, X.518, X.519, X.520, X.521
- Country name
 - C = "AR".
- State or Province Name
 - S = "Ohio".
- Locality Name
 - L = "Edinburgh"
- Common name
 - CN = "Mr. Robin Lachlan McLeod BSc(Hons) CEng MIEE"

X.520 - Tipos de atributos

ATTRIBUTE TYPES

- A Aliased Object Name *
- Authority Revocation List
- B Business Category
- C CA Certificate
- Certificate Revocation List
- **Common Name**
- **Country Name**
- Cross Certificate Pair
- D Description
- Destination Indicator
- F Facsimile Telephone Number
- I International ISDN Number
- K Knowledge Information
- L Locality Name
- M Member
- O Object Class *
- **Organization Name**
- Organizational Unit Name
- Owner

ATTRIBUTE TYPES

- P Physical Delivery Office Name
- Post Office Box
- Postal Address
- Postal Code
- Preferred Delivery Method
- Presentation Address
- R Registered Address
- Role Occupant
- S Search Guide
- See Also
- Serial Number
- **State or Province Name**
- Street Address
- Supported Application Context
- Surname
- T Telephone Number
- Teletex Terminal Identifier
- Telex Number
- Title
- U User Certificate
- User Password
- X X.121 Address

Autoridades Certificantes (CAs)

- Función: certificación de firmas requiere
 - verificación de identidad (procedimiento administrativo)
 - almacenamiento de certificados y numeración
 - mantenimiento de CRLs
 - publicación de directorios de claves públicas
 - confiabilidad / disponibilidad
 - reconocimiento / reputación
- setup de una CA: requiere equipamiento e instalaciones especiales, procedimientos y mecanismos para asegurar *trusted paths*, personal seleccionado especialmente, almacenamiento seguro de la clave privada de la CA

Cadena de confianza

- Julio Iglesias canta mejor que yo
Firmado: Carlos Gardel

Certifico que la firma que antecede es válida y
corresponde a Carlos Gardel
Firmado: Mahatma Ghandi

Certifico que la firma que antecede es válida y
corresponde a Mahatma Ghandi
Firmado: Joe Church



Caso práctico

0.3 Tratamiento de la clave pública



FIUBA

41

Solicitud de certificado

```
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=AR, SP=Buenos Aires, L=Cap. Federal,
           O=Consultora San Gabriel S. A.,
           OU=Depto. Contable, CN=Juan Perez,
           Email=jperez@csg.com.ar
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public Key: (1024 bit)
    Modulus:
      00:b7:96:f9:23:50:66:cf:ff:a1:3d:f9:91:e3:e3:
      ...
      e3:61:98:a2:71:34:78:06:ec:f9:b4:cd:5c:8f:4b:
      c0:97:e2:ac:2a:f6:23:c5:0d
    Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: md5withRSAEncryption
    34:57:8a:c2:57:02:cc:41:d7:0e:f6:c4:00:7f:7e:d9:b4:36:
    ...
    61:59:51:2d:a3:74:c7:57:4e:9d:2a:43:9c:79:e6:4a:cf:b1:
    3c:32
```

FIUBA

42

Caso práctico

0.4 Firma del certificado



Certificado emitido por la CA

```

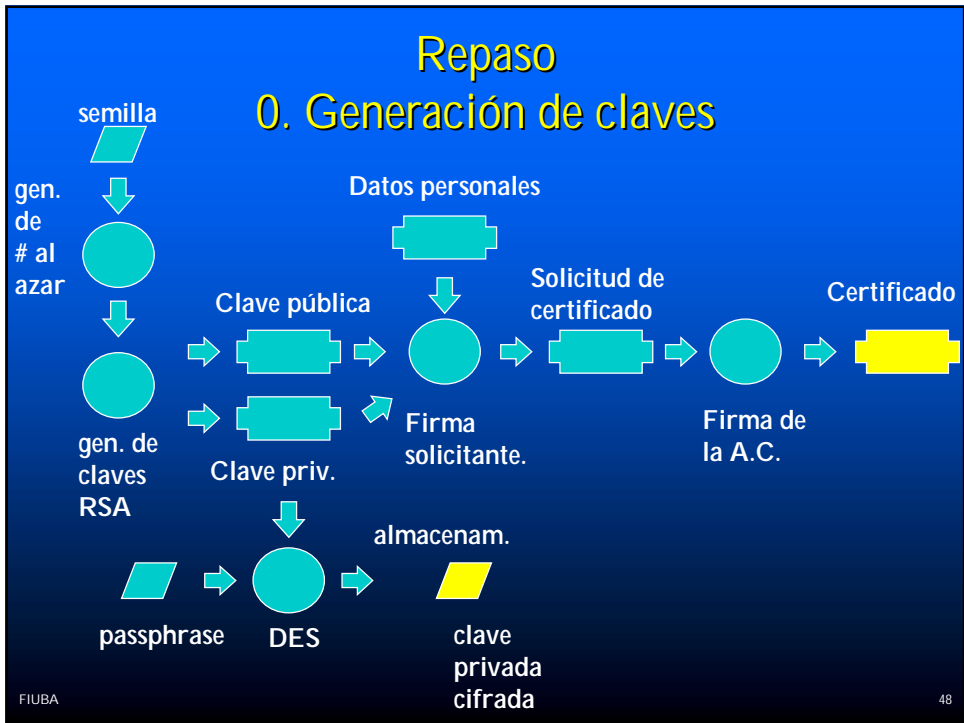
Certificate:
  Data:
    Version: 0 (0x0)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5withRSAEncryption
    Issuer: C=AR, SP=Neuquen, L=Piedra del Aguila,
    O=Trooch Certificados, Ltd.,
    OU=Depto. Certificaciones, CN=Yo-Yo Ma,
    Email=yoyo@trooch.com.ar
    Validity
      Not Before: Oct  9 02:47:53 1996 GMT
      Not After : Oct  9 02:47:53 1997 GMT
    Subject: C=AR, SP=Buenos Aires, L=Cap. Federal,
    O=Consultora San Gabriel S. A.,
    OU=Depto. Contable, CN=Juan Perez,
    Email=jperez@csg.com.ar
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Modulus:
        00:b7:96:f9:23:50:66:cf:ff:a1:3d:f9:91:e3:e3:
        ...
        e3:61:98:a2:71:34:78:06:ec:f9:b4:cd:5c:8f:4b:
        c0:97:e2:ac:2a:f6:23:c5:0d
      Exponent: 65537 (0x10001)
    Signature Algorithm: md5withRSAEncryption
    8b:8e:20:1e:32:02:67:c7:ae:df:50:e9:21:17:48:7b:80:d5:
    ...
    f4:b8:ff:d9:3a:11:3b:49:17:b6
  
```

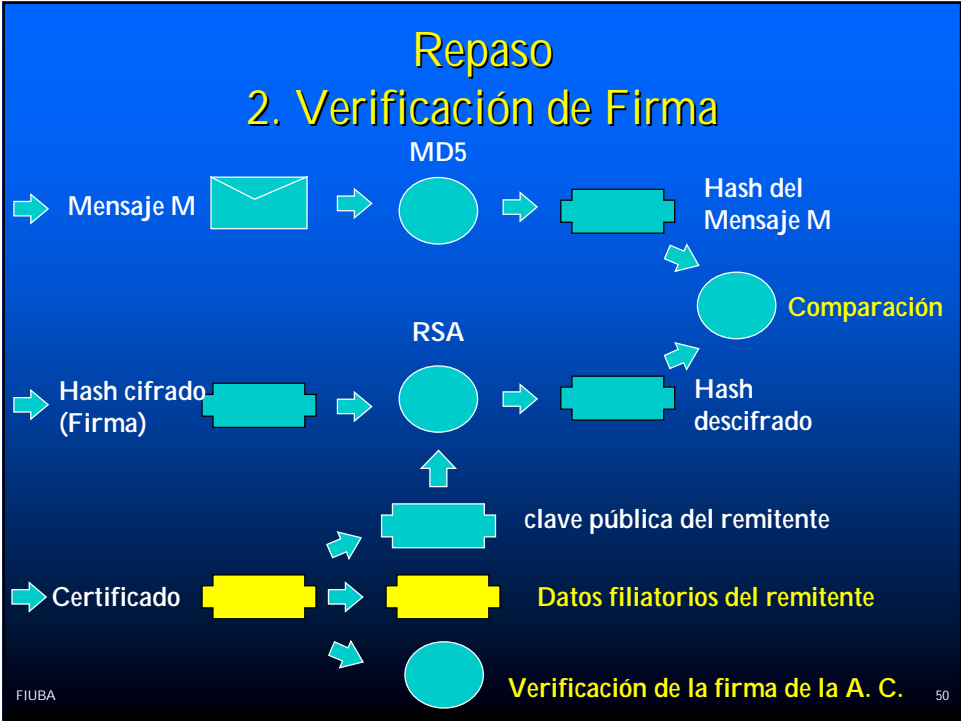
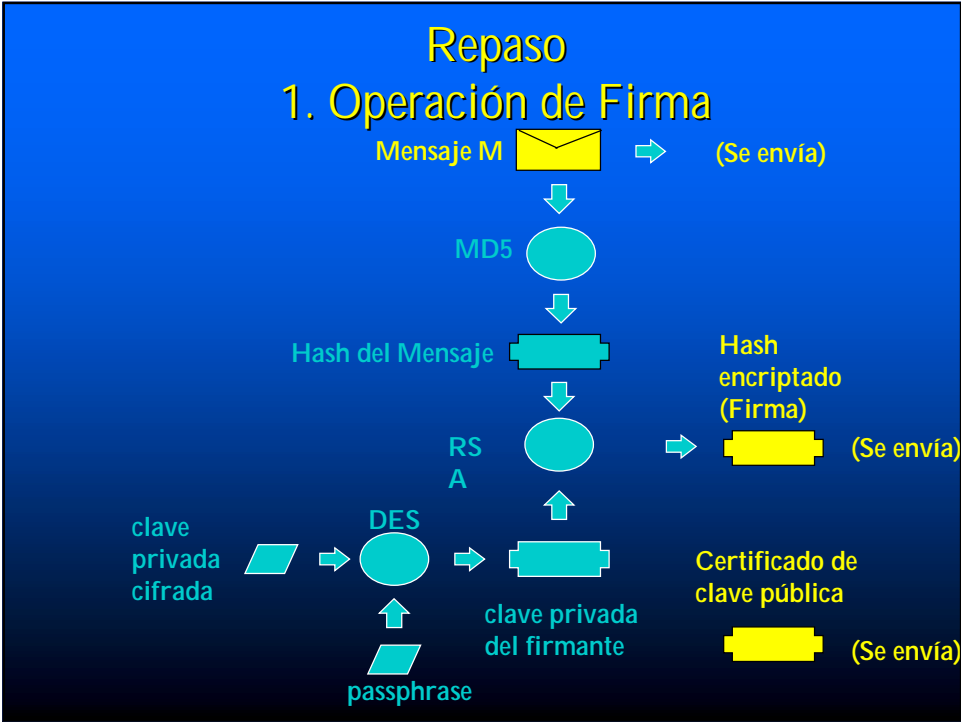
Certificado

```
-----BEGIN CERTIFICATE-----
MIICmTCCAkMCAQEwDQYJKoZIhvcNAQEEBQAwgbyxCzAJBgNVBAYTAkFMSRAwDgYD
VQQIEwdOZXVxdWVumRowGAYDVQQHExFQaWVkcmeGZGVsIEFndWlsYTEiMCAGA1UE
ChMZVHJvb2NoIENlcnRpZmljYWRvcywgTHRkLjEfmB0GA1UECkxMWRGVwdG8uIENl
cnRpZmljYWNpb25lczERMA8GA1UEAxMIWW8tww8gTWEyITAFBgkqhkiG9w0BCQEW
EnlveW9AdHJvb2NoLmNvbS5hcjAeFw05NjEwMDkwMjQ3NTNaFw05NzEwMDkwMjQ3
NTNaMIGzMQswCQYDVQQGEwJBUjEVMBMGA1UECBMMQnV1bm9zIEFpcmVzMRUwEwYD
VQQHEwxDYXAuIEZlZGVyYWxwJTAjBgNVBAoTHEbnbnN1bHRvcmeGgU2FuIEEdhYnJp
ZWwgUy4gQS4xGDAWBgNVBAsTD0RlcHRvLiBDb250YWJsZTETMBEGA1UEAxMKSnVh
biBQZXJleJEGMB4GCSqGSIb3DQEJARYRanBlcmV6QGNzZy5jb20uYXlIwGZ8wDQYJ
KoZIhvcNAQEEBQADgY0AMIGJAoGBALeW+SNQZs//ot35kePjcmHxSMkNXdhyS/wY
ogIAqALWGHoVYi8nqbrHsk+e3Ldpk6UmiuDz6hr3I8j7C50J4vfJ9KngpMjKbFZa
fHEkDufF5DOaUVF/08v5qm7+cbUC8xgXFDHvytSk42GYonE0eAbs+bTNXI9LwJfi
rCr2I8UNAgMBAEwDQYJKoZIhvcNAQEEBQADQCLjIAeMgJnx67fUOkhF0h7gNW3
nW0HyA+szy5O5VdZQv5CBN9E/sm7FWpcWwWX4FTPL4WCRuf0uP/ZOhE7Sre2
-----END CERTIFICATE-----
```

Pero..

- Estos mecanismos sólo “garantizan” la integridad del mensaje, y la relación entre un DN y el poseedor de una clave privada.
- La confianza se translada a la autoridad certificante
- El sistema requiere la consulta online de Listas de Certificados Revocados (CRLs)
- La filtración inadvertida de una clave privada no puede distinguirse de una firma verídica.
- El firmante puede negar la firma denunciando fraudulentamente su pérdida. - Timestamping





3

3. Cripto en la red (y ...)

- **Cripto a nivel aplicación**
 - E-Mail con S/MIME / certs. X.509
- **Cripto a nivel transporte**
 - HTTP, Telnet, FTP, SMTP a través de SSL
- **Cripto a nivel IP**
 - IPSec
- **Cripto a nivel link / físico**
 - encriptadores por hardware

S-MIME - Mensaje Encriptado

Message-ID: <33865AEB.1F95C937@jus.gov.ar>
Date: Sat, 24 May 1997 00:05:15 -0300
From: Alejandro Roman <aroman@jus.gov.ar>
X-Mailer: Mozilla 4.0b4 [en] (Win95; I)
MIME-Version: 1.0
To: aroman@jus.gov.ar
Subject: Prueba mail **encriptado**
Content-Type: application/x-pkcs7-mime; name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: S/MIME Encrypted Message

MIAGCSqGSIB3DQEHA6CAMIACAQAxgc8wgcwCAQAwDjBimREwDwYDVQQHEwhJbnRlcm5ldDEX
MBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNDAYBgNVBAsTK1ZlcmlTaWduIENsYXNzIDEGQ00Eg
LSBJbmRpdmlkdWFsIFNlYnNjcmlIZXICeGLOAdwiI2PK5woNBB2MQCwwDQYJKoZIhvcNAQEB
...
HXtLw4oV/yAEIMkuFMWafnaAktHm14jTbqlKfhQYUwnmnLpP1wEpdP2DBDgF4kZhcncBlQvdo
47ivOgAFggwAHoqZmEfAv5FKATGB5jBDLlNRBTLjsjde+OUWyAeSUL6OTF84oAQwFu6gheXk
9nqayxD+izJIHSYrgSYGoXs8r/bdB24YY+0QO2tBTsw+NsHv3kSp58NfBAhcMh jphUhtqgAA
AAAAAAAAAA=

FIUBA

53

S-MIME - Mensaje firmado

To: admin@jus.gov.ar
Subject: Prueba e-mail **firmado digitalmente**
Content-Type: **multipart/signed**; protocol="application/x-pkcs7-
signature"; micalg=shal; boundary="-----
msEB8551806A73E1DCEF974304"
This is a cryptographically signed message in MIME format.

-----msEB8551806A73E1DCEF974304
Content-Type: **text/plain**; charset=iso-8859-1
Content-Transfer-Encoding: 8bit

**Puedo decir que no estuve perdido ni una sola vez, pero una vez estuve
muy confundido durante tres días.**

-- Daniel Boone

-----msEB8551806A73E1DCEF974304
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: **attachment**; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIIQmgYJKoZIhvcNAQcCoIIQizCCEIcCAQExCzAJBgUrDgMCGGUAMAsGCSqGSIB3DQEHAaC
C

...
s6YXZ8XE3JCFsWsGu/ZOx3Db8q0L1GFxrczA1zsNN0HrIePbKXPHkblq

FIUBA

-----msEB8551806A73E1DCEF974304--

54

Verificación de firma digital



3. Cripto en la red

- Cripto a nivel aplicación
 - E-Mail con S/MIME / certs. X.509
- Cripto a nivel transporte
 - HTTP, Telnet, FTP, SMTP a través de SSL
- Cripto a nivel IP
 - IPsec
- Cripto a nivel link / físico
 - encriptadores por hardware

SSL

(secure sockets layer)

- Protocolo independiente de la plataforma y de las aplicaciones
- Base para transacciones comerciales usando el WWW; administración remota, etc.
- Opera entre la capa de aplicación y la de transporte (TCP)



SSL

- Es un protocolo para negociar los parámetros criptográficos de una sesión, e implementar los mecanismos de seguridad necesarios para lograr transferencias seguras
 - autenticación mutua
 - privacidad de datos
 - integridad de datos
- Transparente, "Simple"
- permite utilizar diferentes algoritmos criptográficos (cipher suites) según las necesidades, incluyendo Fortezza, SHA

SSL: Autenticación mutua

- Objeto: establecer un *trusted path* entre interlocutores
- Un server debe autenticarse ante un cliente
- Un cliente puede autenticarse ante un server

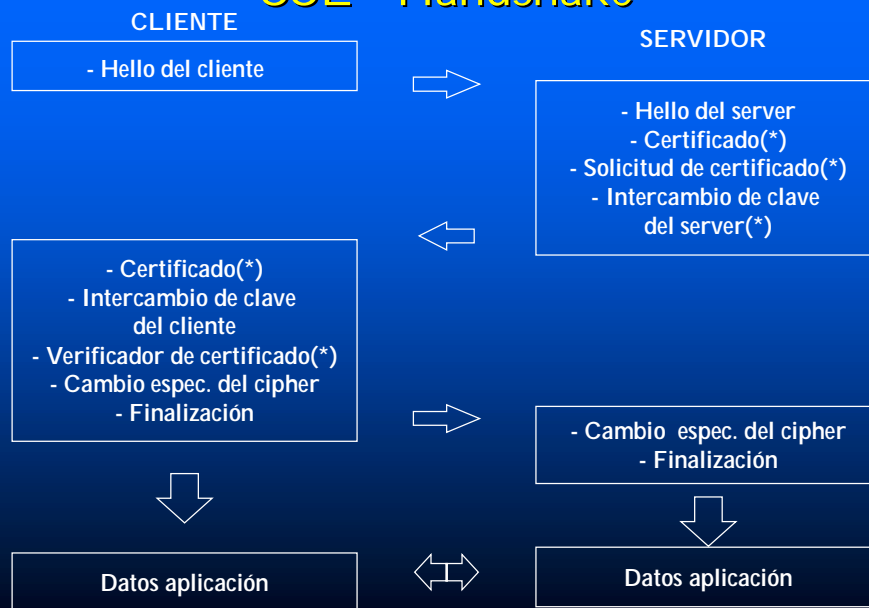
SSL 3.0 - Subcapas

- Handshake layer
 - Aquí se producen los mensajes de negociación. Todos incluyen una MAC; el orden de los mensajes es absoluto
- Record layer
 - Fragmentación (2^{14} max. long. bloque)
 - Compresión
 - Autenticación de mensaje (MAC)
 - Cifrado
- Alert layer
 - errores de finalización
 - errores de secuencia de mensaje
 - MACs incorrectas
 - errores en los certificados

Sesiones y conexiones

- Estado de una **sesión**
 - identificador
 - certificado del corresponsal
 - metodo de compresión
 - especificación del *cipher*
 - master secret
 - is_resumable
- Estado de una **conexión**
 - random de server y cliente
 - server write MAC secret
 - client write MAC secret
 - server write key
 - client write key
 - IVs (uno por cada clave)
 - números de secuencia

SSL - Handshake



Master secret

pre-master secret
↓
MASTER SECRET
(48 bytes)

- client write MAC secret
- server write MAC secret
- client write key
- server write key
- client write IV
- server write IV

Cipher suites

- Las entidades SSL negocian la suite de mecanismos criptográficos que utilizarán en la sesión
- El protocolo puede incorporar nuevas suites a medida que éstas aparezcan
- Las suites "exportables" tienen claves cortas, debido a las restricciones del ex-ITAR (EEUU)

```

CONNECTED
depth=0 /C=AR/CN=Alejandro Roman/Email=aroman@jus.gov.ar
verify error:num=23:self signed certificate
verify return:1
Server certificate
-----BEGIN CERTIFICATE-----
MIIBhjCCATACAQAwdQYJKoZIhvcNAQEEBQAwtjELMAkGA1UEBhMCQVIXGDAWBgNV
...
HaOBuOIpCoz99Q==
-----END CERTIFICATE-----
subject=/C=AR/CN=Alejandro Roman/Email=aroman@jus.gov.ar
issuer=/C=AR/CN=Alejandro Roman/Email=aroman@jus.gov.ar
---
Ciphers common between both SSL endpoints:
RC4-MD5          EXP-RC4-MD5      RC2-CBC-MD5
EXP-RC2-CBC-MD5 IDEA-CBC-MD5     DES-CBC-MD5
DES-CBC-SHA     DES-CBC3-MD5    DES-CBC3-SHA
SSL-Session:
  Cipher       : RC4-MD5
  Session-ID: 5AA0D397D313D75EE0C3A38D7BCE1892
  Master-Key: F9BC891E511A00DC63E39545BA7C7CAD
  Key-Arg      : None
j1j1k1k1kj

```

Transacciones comerciales seguras Web Servers seguros

- El server debe presentar a los clientes (browsers) su certificado, firmado por una CA.
 - se genera un par de claves para el server.
 - La clave privada se encripta y almacena; con la pública y el DN del server se genera un *request X.509*
 - El *request* se envía a la CA
 - la CA verifica, y devuelve un certificado X.509 firmado
 - El certificado se instala en el server.

Transacciones comerciales seguras Web Servers seguros

- Una persona, utilizando el browser genera sus claves
- el browser encripta la clave privada y la guarda
- el browser, con la pública genera un certificate request, que envía a la AC.
- Luego, obtiene un certificado firmado por la AC.
- El browser guarda el certificado junto con la clave privada en un objeto pkcs12 (interoperabilidad!)
- Al requerir un recurso, si el server lo solicita, el browser envía el certificado (fase de handshake de SSL) para autenticarse ante el server.

4

PKI y Autoridades Certificantes

- Qué datos incluyen en los certificados que firman?
- Certificados de firma (relacionan clave pública con identidad)
- Certificados de Atributos (relacionan identidad con atributos)
Ej.:
Juan Pérez,
Director de Coordinación de Gestión Ejecutiva, Ministerio de Gobierno, Salud, Educación y Justicia

Autoridades Certificantes

- Qué procedimientos utilizan para resolver la emisión de un certificado?
 - Facilidad/rapidez
 - Costos
 - Seguros
- Qué componentes técnicos deben utilizar?
- Cómo hacen disponibles a las CRLs?
- Debe existir una "Habilitación"?
- Quiénes las auditan?