UAEM | Universidad Autónoma del Estado de México

Seguridad en Redes

CENTRO UNIVERSITARIO UAEM ZUMPANGO

UNIDAD III

CRIPTOGRAFÍA Y AUTENTICACIÓN

OBJETIVO:

Identificar los elementos de seguridad y el ciclo de vida de las operaciones y las políticas de seguridad.

INTRODUCCIÓN (1/3)

Criptografía

- Criptografía viene de la palabra griega *crypt* que significa oculto y *graphy* que se refiere a escritura. Entonces criptografía significa **escritura oculta**.

- Formalmente, criptografía es la disciplina que estudia las técnicas matemáticas relacionadas a la seguridad de la información, que provee los servicios de confidencialidad, integridad de los datos, autenticación y no rechazo.

INTRODUCCIÓN (2/3)

Criptoanálisis y criptología

- El **criptoanálisis** se refiere al estudio de la escritura oculta, para descubrir el mensaje secreto.

- La **criptología** es el estudio de la escritura oculta, para crear técnicas que permitan ocultar la información.

INTRODUCCIÓN (3/3)

Primitivas criptográficas

- **Función de cifrado** y su inverso la **función de descifrado**.
- **Firma digital** y su inverso la **verificación de la firma**.
- **Función picadillo** (**hash**).

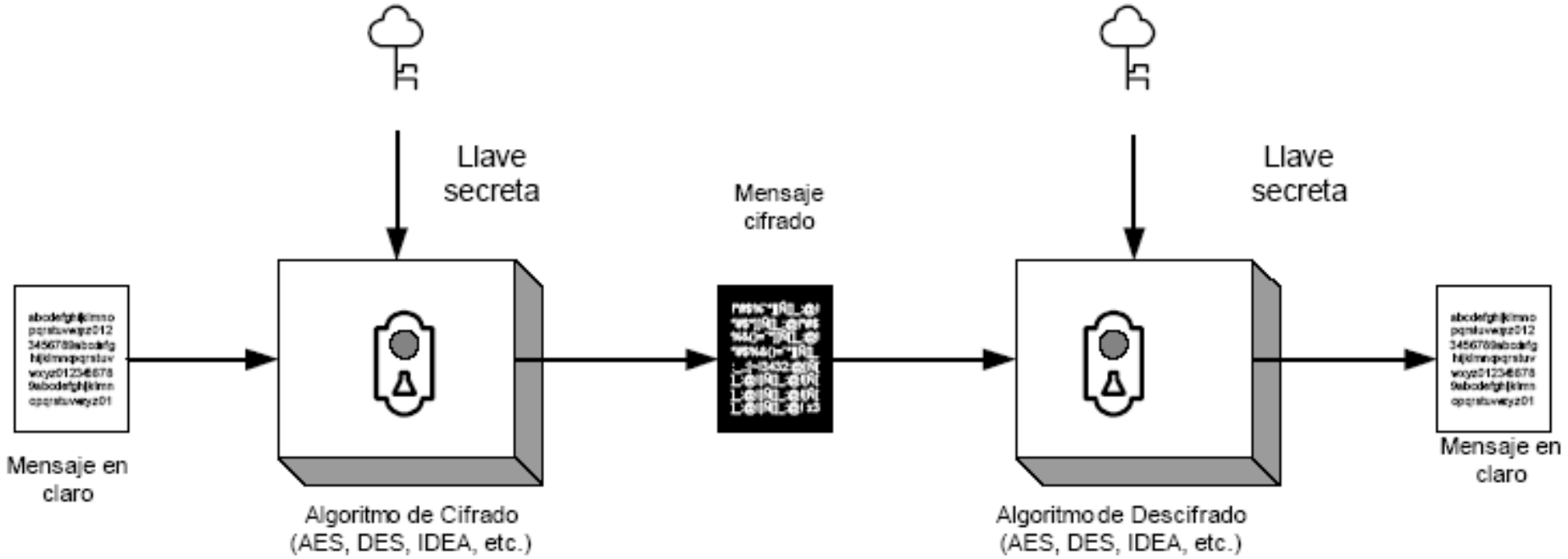
CLASIFICACIÓN DE CIFRADO/DESCIFRADO (1/7)

Existen dos categorías en los que se puede clasificar los métodos de cifrado/descifrado:

- **Cifradores simétricos o criptografía de llave privada.**
- **Cifradores asimétricos o de llave pública.**

CLASIFICACIÓN DE CIFRADO/DESCIFRADO (2/7)

Cifradores simétricos o criptografía de llave privada



CLASIFICACIÓN DE CIFRADO/DESCIFRADO (3/7)

Cifradores simétricos o criptografía de llave privada

Ventajas

- Pueden diseñarse para cifrar grandes cantidades de información.
- Usan llaves más pequeñas que los cifradores asimétricos.
- Puede usarse como primitivas para para la construcción de generadores de números pseudoaleatorios, funciones hash, firmas digitales.
- Pueden combinarse para construir cifradores más fuertes.

CLASIFICACIÓN DE CIFRADO/DESCIFRADO (4/7)

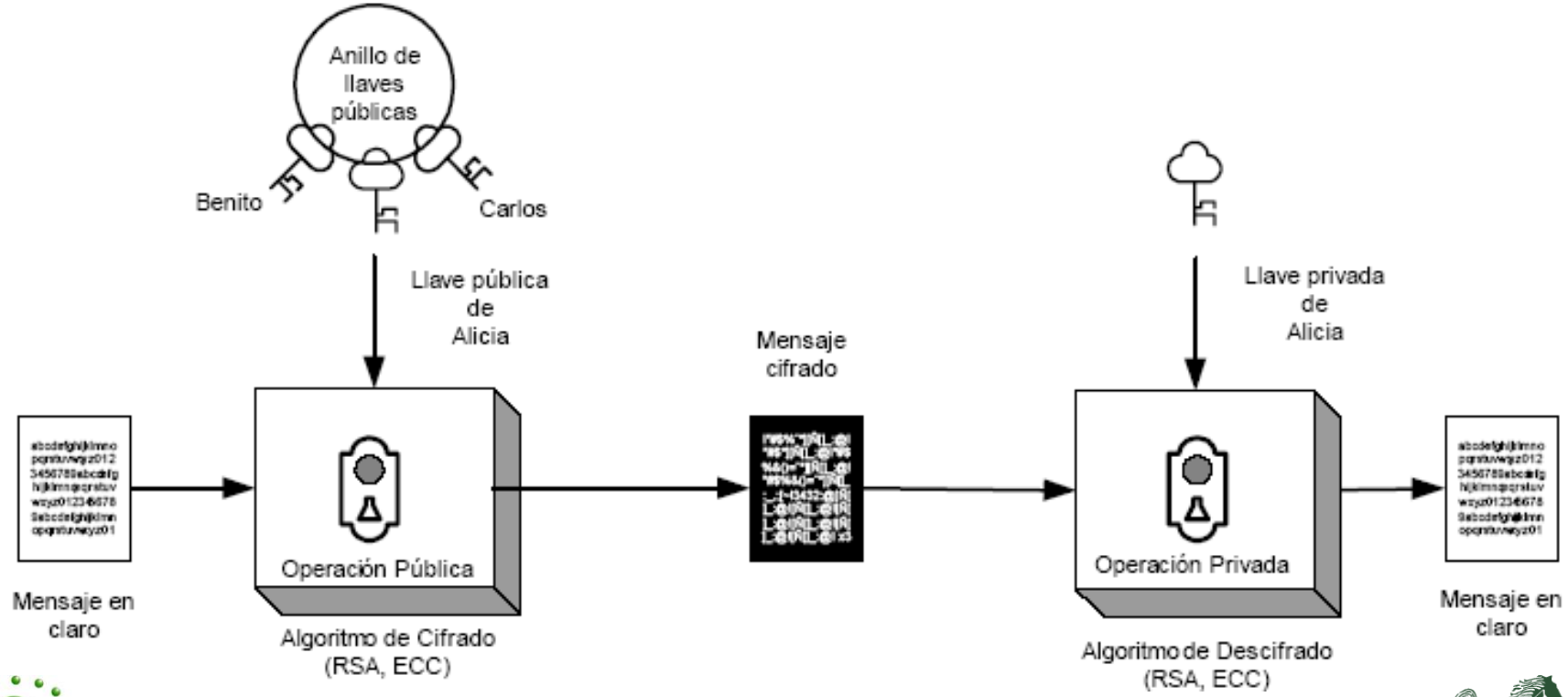
Cifradores simétricos o criptografía de llave privada

Desventajas

- La llave debe permanecer secreta entre las entidades.
- En una red grande se necesita administrar muchas llaves. En un sistema con *n* usuarios se necesitan $\frac{n(n+1)}{2}$ llaves.
- Es recomendable cambiar frecuentemente la llave usada. Idealmente una llave por sesión.

CLASIFICACIÓN DE CIFRADO/DESCIFRADO (5/7)

Cifradores asimétricos o de llave pública



CLASIFICACIÓN DE CIFRADO/DESCIFRADO (6/7)

Cifradores asimétricos o criptografía de llave pública

Ventajas

- Solamente la llave privada debe estar guardada en secreto.
- La administración de las llaves en una red requiere la presencia de una Tercera Entidad de Confianza.
- Las llaves privada y pública pueden durar varias sesiones o incluso varios años.
- Ofrecen mecanismos eficientes de firma digital.
- En una red grande, el número de llaves necesarias puede ser considerablemente más pequeño que en un escenario simétrico.

CLASIFICACIÓN DE CIFRADO/DESCIFRADO (7/7)

Cifradores asimétricos o criptografía de llave pública

Desventajas

- El tiempo de ejecución de los métodos de cifrado de llave pública son considerablemente más lentos que los esquemas de llave simétrica.
- El tamaño de las llaves son mucho más grandes.
- El tamaño de la firma digital usando el esquema de llave pública es grande a comparación con las etiquetas de autenticación de datos que se proveen con las técnicas de llave simétrica.

RSA (1/8)

- RSA (Rivest, Shamir y Adleman) es un algoritmo de cifrado asimétrico desarrollado en el año 1977 por los anteriormente citados.

- Se basa en escoger 2 números primos grandes elegidos de forma aleatoria y mantenidos en secreto.

- La principal ventaja de este algoritmo desde el punto de vista de seguridad radica en la dificultad a la hora de factorizar números grandes.

RSA (2/8)

- La idea del algoritmo es la siguiente:

  Cifrado

$$c \equiv m^e \bmod n$$

  Descifrado

$$m \equiv c^d \bmod n$$

RSA (3/8)

- Generación de llaves:

1. Tomamos 2 números primos *p* y *q*. Estos tienen que ser aleatorios e impredecibles. Importante impredecibles, porque un proceso puede ser perfectamente aleatorio, pero si se conoce, se puede predecir los valores, y por tanto, resultaría en una baja seguridad.

2. Calculamos $n = p*q$.

RSA (4/8)

- Generación de llaves:

3. Calculamos φ(n). La función φ de Euler se define como el número de enteros positivos menores o iguales a n y coprimos con n (dos números son coprimos si no tienen ningún divisor común distinto 1 o -1. La función tiene las siguientes propiedades:
   - φ(1)=1.
   - φ(p)= p - 1 si p es primo.
   - φ(p^k)= (p - 1)*p^(k - 1) si p es primo y k un número natural.
   - φ(m*n)=φ(m)φ(n) si m y n son primos.

De esta forma nos queda que para nuestro n=p*q:

$$\varphi(n)=(p - 1)*(q -1)$$

RSA (5/8)

- Generación de llaves:

4. Escogemos un número e menor que φ(n) y que sea coprimo con φ(n). Este número será dado a conocer como exponente de la clave pública.

5. Obtenemos un número d mediante aritmética modular tal que d = e^(-1) mod(φ(n)) o lo que es lo mismo (d*e)-1 tiene que ser divisible por φ(n).

   De esta forma tenemos la clave pública formada por (n,e) y la privada formada por (n,d).

RSA (6/8)

Ejemplo:

p = 61	nº primo privado
q = 53	nº primo privado
n = p*q = 3233	producto p×q
e = 17	exponente público
d = 2753	exponente privado

RSA (7/8)

Ejemplo:

La clave pública (e, n). La clave privada es (d, n). La función de cifrado e

$$c = m^e \bmod n = m^{17} \bmod 3233$$

Donde m es el texto sin cifrar. La función de descifrado es:

$$m = c^d \bmod n = c^{2753} \bmod 3233$$

Donde c es el texto cifrado. Para cifrar el valor del texto sin cifrar 123, nosotros calculamos:

$$c = 123^{17} \bmod 3233 = 855$$

RSA (8/8)

Ejemplo:

Para descifrar el valor del texto cifrado, nosotros calculamos:

$$m = 855^{2753} \bmod 3233 = 123$$

DIFFIE HELLMAN (1/4)

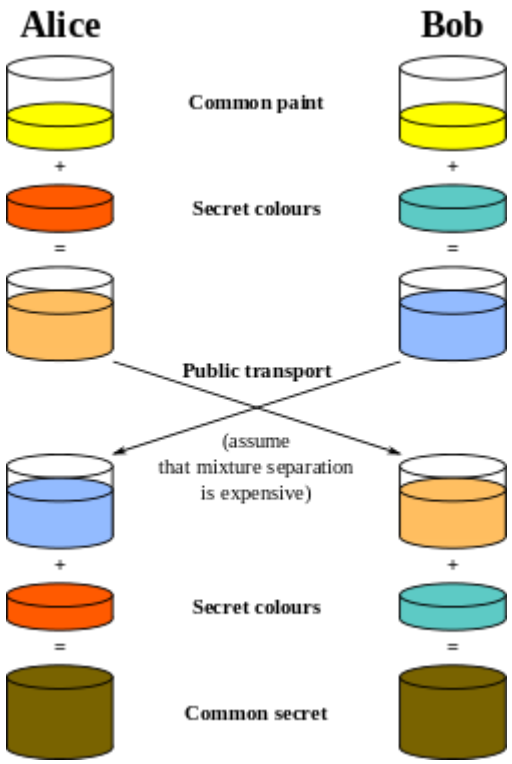
El intercambio de llaves Diffie Hellman en un protocolo para el intercambio seguro de llaves criptográficas sobre un canal público (inseguro), sin haber tenido un contacto previo.

La llave puede ser usada puede ser usada para cifrar subsecuentes.

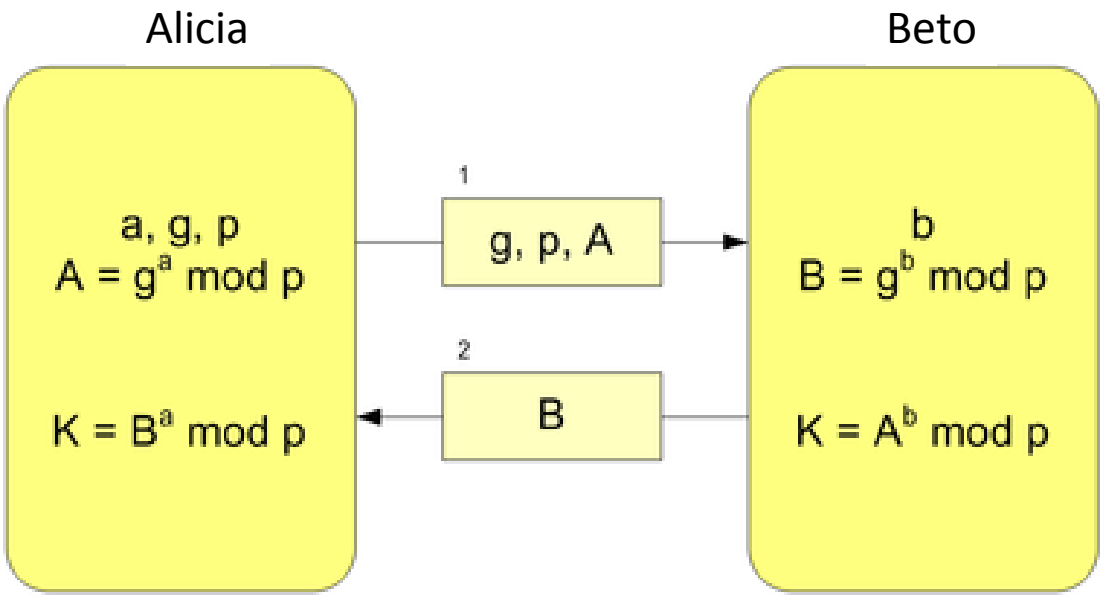
El esquema fue publicado por **Whitfield Diffie** y **Martin Hellman** en 1976.

El sistema se basa en la idea de que dos interlocutores pueden generar conjuntamente una llave compartida sin que un intruso que esté escuchando las comunicaciones pueda llegar a obtenerla.

DFFIE HELLMAN (2/4)



DIFFIE HELLMAN (3/4)



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

DIFFIE HELLMAN (4/4)

- Alicia y Beto acuerdan usar un número primo $p = 23$ y un generador $g = 5$ (el cual es una raíz primitiva módulo 23).
- Alicia selecciona un entero secreto $a = 6$, y envía a Beto $A = g^a \bmod p$
  - $A = 5^6 \bmod 23 = 8$
- Beto selecciona un entero secreto $b = 15$, y envía a Alicia $B = g^b \bmod p$
  - $B = 5^{15} \bmod 23 = 19$
- Alicia procesa $s = B^a \bmod p$
  - $s = 19^6 \bmod 23 = 2$
- Beto procesa $s = A^b \bmod p$
  - $s = 8^{15} \bmod 23 = 2$
- Alicia y Beto ahora comparten un secreto (el número **2**).

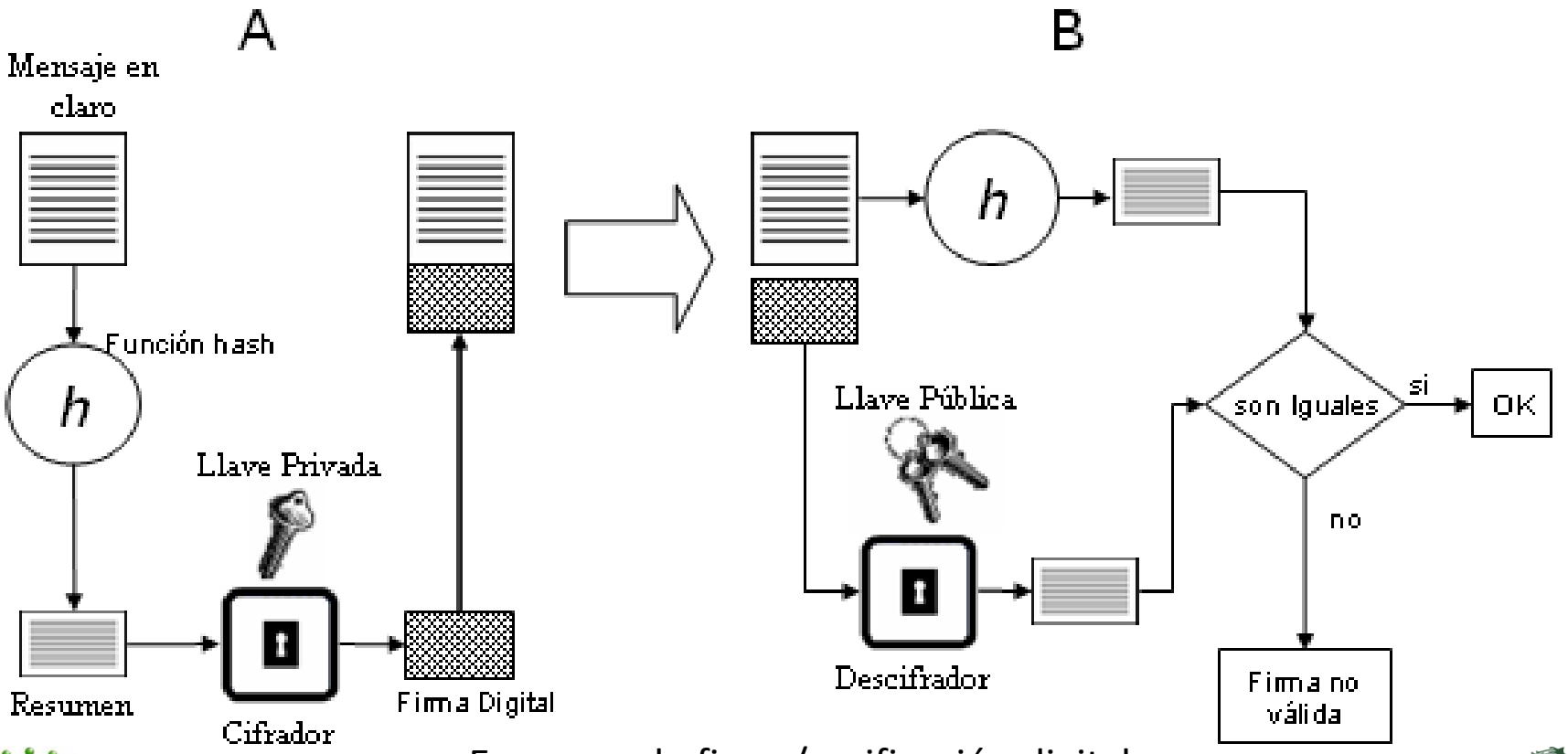
ALGORITMO DE FIRMA DIGITAL (1/6)

- Las firmas digitales proveen a una entidad un medio para enlazar su identidad a una pieza de información.

- El proceso de firma se hace con base en la utilización de un cifrador de llave pública.

- Al mensaje se le aplica una función *Hash* y se firma utilizando la llave privada. El proceso de verificación se realiza con la llave pública.

ALGORITMO DE FIRMA DIGITAL (2/6)



Esquema de firma/verificación digital

ALGORITMO DE FIRMA DIGITAL (3/6)

- En 1991 el Instituto Nacional de Estándares de Estados Unidos (NIST) propuso el **algoritmo de firma digital** (DSA) y se adoptó como estándar en 1994.

- **DSA** en un esquema de firma digital con huella o digesto, es decir se firma el mensaje digerido resultado de aplicar una función *hash*.

- Para la firma y verificación DSA genera un par de llaves, una llave privada y una llave pública.

ALGORITMO DE FIRMA DIGITAL (4/6)

Generación de llaves

Para generar las llaves se debe seguir una fase de inicialización:

1. **A** encuentra un primo q de longitud de 160 bits y elige un primo p tal que $q|p-1$
2. Sea g una raíz primitiva mod p y sea $\alpha \equiv g^{(p-1)/q} \bmod p$. Entonces $\alpha^q \equiv 1 \bmod p$.
3. **A** elige un secreto a tal que $1 \leq a \leq q-1$ y calcula $\beta \equiv \alpha \bmod p$.
4. A publica (p,q,α,β) y mantiene en secreto a.

ALGORITMO DE FIRMA DIGITAL (5/6)

A firma un mensaje

1. Selecciona un número entero aleatorio k tal que $0 < k < q-1$. k se mantiene en secreto.
2. Calcular $r \equiv (\alpha^k \bmod p) \bmod q$.
3. Calcular $s \equiv k^{-1} (m + ar) \bmod q$.
4. La firma de A para m es (r,s). Esta firma se envía a B junto con m.

ALGORITMO DE FIRMA DIGITAL (6/6)

B verifica la firma del mensaje

1. Obtener los datos públicos de A, (p,q,α,β)
2. Calcular $u_1 \equiv s^{-1}\, m \bmod p$ y $u_2 \equiv s^{-1}\, r \bmod q$.
3. Calcular $v \equiv (\alpha^{u1}\, \beta^{u2} \bmod p) \bmod q$.
4. Se acepta la firma si y sólo si $v = r$.

REFERENCIAS (1/2)

1. Stallings, W. “Fundamentos de seguridad en redes: aplicaciones y estándares” (2ª Ed). Pearson-Prentice Hall, 2004.
2. Stallings, W. “Network Security Essentials – Applications and Standars” 3a edición.
3. F. Rodríguez-Henríquez, N. A. Saqip y A. Díaz-Pérez and C. K. Koç, Cryptographic Algorithms on Reconfigurable Hardware (Signals and Communication Technology), Springer-Verlag New York, Inc. 2006.
4. Carracedo, “J. Seguridad en Redes Telemáticas”. Mc Graw Hill, 2004.
5. Elizabeth D. Zwicky, Simon Cooper “Building Internet Firewalls” (2ª Ed). O’Reilly & Associates,2000.
6. Housley, R., Ford, W. and Solo, D. Internet X.509 Public Key Infrastructure. “Certificate and CRL Profile.” RFC 3280, 2002.
7. McClure, S., Scambray, J. and Kurtz, G. “Hackers. Secretos y soluciones para la seguridad de redes.” McGraw-Hill, 2000.

REFERENCIAS (2/2)

8. McClure, S., Scambray, J. and Kurtz, G. “Hackers 2. Secretos y soluciones para la seguridad de redes.” McGraw-Hill, 2001.
9. McClure, S., Scambray, J. and Kurtz, G. “Hackers 3. Secretos y soluciones para la seguridad de redes.” McGraw-Hill, 2002
10. Garfinkel, S., Spafford, G. “Practical UNIX & Internet security” (2ª Ed). O’Reilly & Associates Inc. Abr. 1996
11. McClure, S., Scambray, J. and Kurtz, G. “Hacking Exposed. Network Security Secrets and Solutions” (Third Edition). McGraw-Hill, 2001.
12. Pastor, J. y Sarasa, M.A. “Criptografía digital: fundamentos y aplicaciones.” Zaragoza: Prensas Universitarias, 1998.