Criptografía

Profesor: Melvin Fernández Ch.

Video 9

fidélitas
Virtual

fidélitas Virtual

Criptografía simétrica y asimétrica

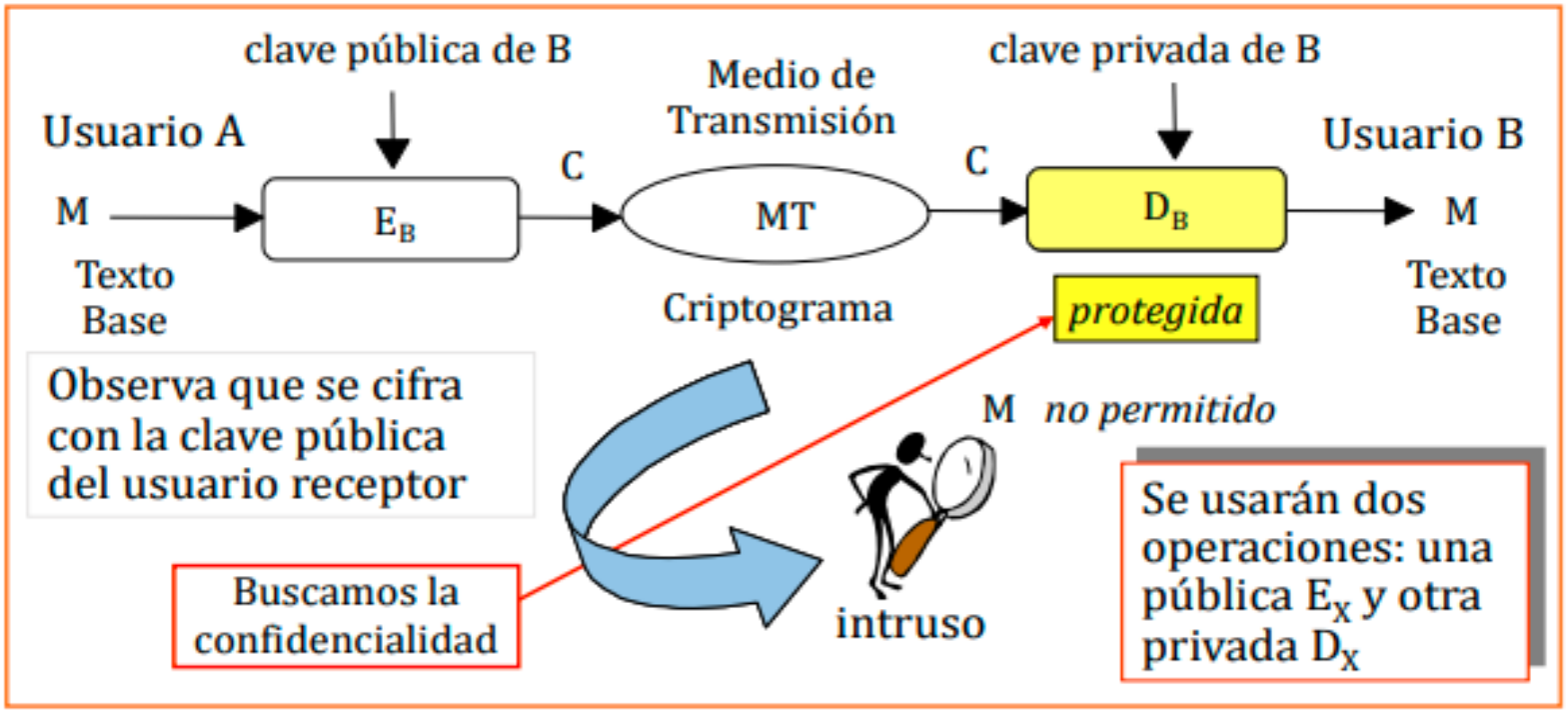
Módulo: 3

Generalidades cifra asimétrica

- Una clave se mantiene privada y la otra se hace pública.

- Dependiendo de la aplicación, el emisor usa su clave privada, la clave pública del receptor o ambas para realizar algún tipo de función criptográfica.

Confidencialidad en cifra asimétrica



$$C = E_B(M)$$

$$M = D_B(C) = D_B(E_B(M))$$

E_B y D_B son operaciones con inversos dentro del módulo de cifra del usuario B

Algoritmo Diffie - Hellman

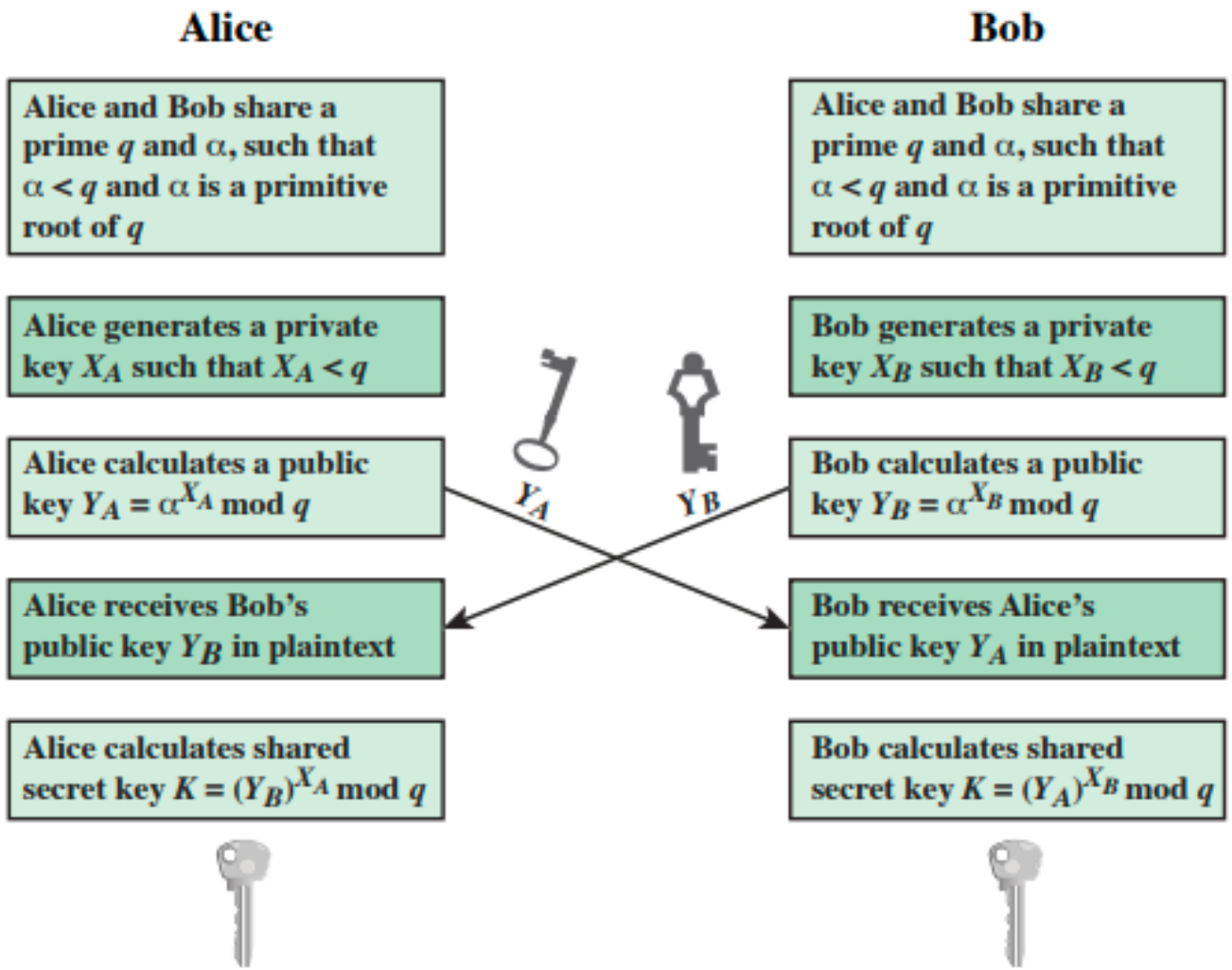
- Primer algoritmo de clave pública que fue publicado:
  - “New Directions in Cryptography”, IEEE Trans. Information Theory, 1976

- Su propósito es permitir a dos partes derivar una clave secreta de forma segura que pueda ser después usada para cifrar mensajes.

- El algoritmo se limita al intercambio de claves.

- Su seguridad depende de la dificultad de calcular logaritmos discretos.

Algoritmo Diffie - Hellman



Algoritmo RSA

- Uno de los primeros esquemas de clave pública desarrollado en 1977 por Ron Rivest, Adi Shamir y Len Adleman en el MIT.
  - "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems".
  - Uno de los esquemas más aceptados e implementados.

- Cifrado de bloque en el que el texto plano y cifrado son enteros entre 0 y n - 1 para un n.

Algoritmo RSA

- La seguridad se basa en dos problemas matemáticos, para los que no existe un algoritmo eficiente:
  - Factorización de enteros (descomposición en factores primos)
  - El problema RSA (revertir la operación de cifrado RSA)

- En general, se supone que RSA es seguro si n es suficientemente grande.

Comparación simétrico - asimétrico

fidélitas Virtual

TIPO DE CIFRA	VENTAJAS	DESVENTAJAS
SIMÉTRICA	• Alta velocidad o tasa de cifra MB/s • Eficiente para su uso grupos reducidos (redes pequeñas) al necesitar una sola clave • Posee una infraestructura sencilla • Las claves pueden ser pequeñas, de tan solo unas centenas de bits	• Es necesario compartir una clave por medios que pueden ser no seguros pues no permite un intercambio de clave • Si se compromete la clave, se compromete toda la comunicación • No permite autenticar a los usuarios pues una clave la pueden usar varios usuarios • Elevado número de claves a recordar
ASIMÉTRICA	• Número de claves reducido, dos claves por usuario y sólo una secreta a recordar • Seguridad computacional de la clave privada • No es necesario transmitir la clave privada entre emisor y receptor • Permite un intercambio de valor secreto de forma computacionalmente segura • Permite autenticar a los usuarios	• Baja velocidad o tasa de cifra KB/s • La generación de claves requiere de un proceso diferente para cada algoritmo • Las claves deben ser muy grandes • Necesidad de una gran infraestructura de clave pública • Necesidad de una tercera parte de confianza o Autoridad de Certificación

Gracias

fidélitas Virtual