UT5: Sistemas de identificación. Criptografía. Parte2

2º Curso CFGM SMR

Índice.

Repaso …

- Hay dos grandes grupos de algoritmos de cifrado:

✓ **Simétricos o de clave simétrica o privada**: una ***única clave*** en el proceso de *cifrado* como en *descifrado*.

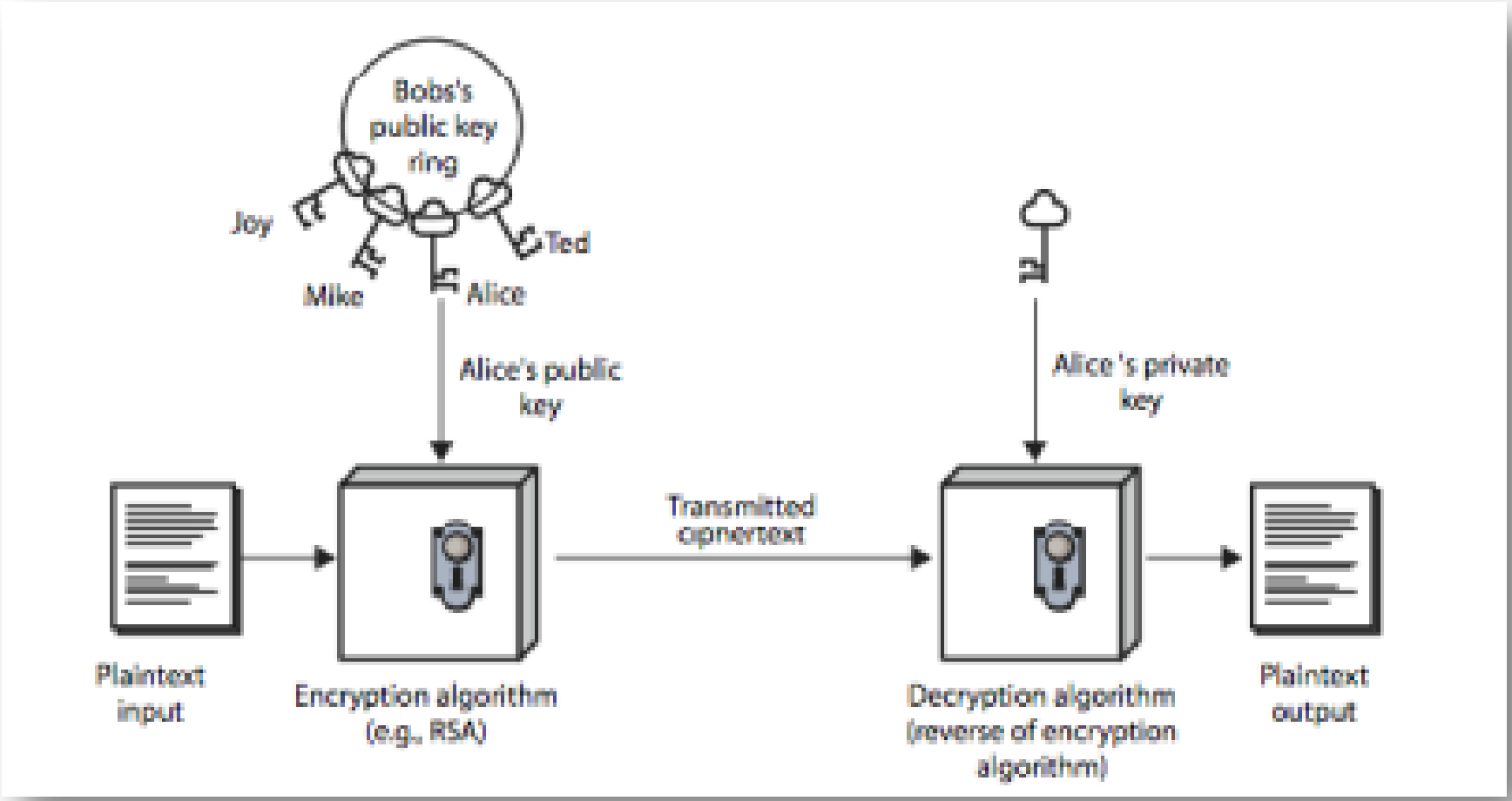
✓ **Asimétricos o de clave asimétrica o pública**: ***dos claves:*** una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Estos forman el núcleo de las técnicas de cifrado modernas: certificados digitales, firma digital, DNIe.

5.2. Tipos de algoritmos de cifrado.

- *Criptografía asimétrica:* **Fundamentos.**

- ✓ Cada usuario del sistema ha de poseer una pareja de claves:
  - **Clave privada:** custodiada por propietario y no se dará a conocer.
  - **Clave pública:** conocida por todos los usuarios.
- ✓ Pareja de claves complementaria: ***lo que cifra una, solo lo puede descifrar la otra y viceversa.***
- ✓ Se desarrollo para tratar dos problemas clave:
  - Firma digital: cómo verifico que un mensaje llega intacto y el que lo envía es realmente quien dice ser?
  - Distribución de claves, intercambio de claves de sesión.
  - Cifrado: para proporcionar confidencialidad.
- ✓ Los inventores: Diffie & Hellman en 1976.

5.2. Tipos de algoritmos de cifrado.



5.2. Tipos de algoritmos de cifrado.

- *Criptografía asimétrica:* **Claves.**

✓ Fácil computacionalmente de cifrar/descifrar cuando se conocen las claves.

✓ Sin embargo, computacionalmente difícil/imposible obtener clave descifrado a partir de la de cifrado y del algoritmo.

✓ Se usan funciones unidireccionales con trampa: factorización de números primos.

✓ Son reversibles: cualquiera de las dos claves se pueden usar para cifrar y descifrar:

- Si cifro con clave pública, descifro con clave privada. (confidencialidad + integridad)
- Si cifro con clave privada, descifro con clave pública. (no repudio+autenticidad de emisor)

5.2. Tipos de algoritmos de cifrado.

- *Criptografía asimétrica:* **Algoritmos.**

- ✓ Diffie-Hallman
- ✓ RSA
- ✓ DSA
- ✓ ElGamal

5.2. Tipos de algoritmos de cifrado.

- *Criptografía asimétrica:* **Desventajas.**

- La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes **desventajas**:
  - ✓ Misma longitud de clave y mensaje **mayor tiempo de proceso**.
  - ✓ Las **claves deben ser de mayor tamaño** que las simétricas: Mínimo 1024 bits.
  - ✓ El **mensaje cifrado ocupa más espacio** que el original.

5.2. Tipos de algoritmos de cifrado.

Comparativa: claves.

- **Cifrado simétrico**
  - Para n participantes, entran en juego
    - n * (n-1) / 2 claves
- **Cifrado asimétrico**
  - Para n participantes, entran en juego
    - 2 * n claves

EJEMPLO

Para n = 100 (100 participantes)

- **Simétrico:** 100x99/2 = 4950 claves.
- **Asimétrico:** 2x100 = 200 claves

Clave Pública de Ana

Clave Pública e Ana

Destinatario del mensaje

Privada de Ana

Pública de Ana

Todos conocen la clave pública

Sólo Ana podrá leer sus mensajes.

Clave Pública de Ana

Clave Privada de Ana

Clave Pública de Ana

Clave Privada de Ana

Usan cl. publica para cifrar. Cualquiera le puede enviar mensajes.

5.2. Tipos de algoritmos de cifrado.

- *Clave asimétrica: Claves de **destinatario***:
- Si uso una clave pública para cifrar, usaré clave privada para descifrar.
  - Proporciona:
    - Confidencialidad: sólo el destinatario tiene la clave privada y podrá descifrar.
    - Integridad: si el mensaje es alterado, no se podrá descifrar.
  - No proporciona:
    - Autenticación: autenticidad del emisor, cualquier tiene la clave pública.
    - No repudio: el emisor puede negar haber sido él quien lo envió. Cualquiera tiene la clave pública.

5.2. Tipos de algoritmos de cifrado.

- *Clave asimétrica: Claves de **origen***:
- Si uso una clave privada para cifrar, usaré clave pública para descifrar.
  - Proporciona:
    - Integridad.
    - Autenticación: sólo el origen pudo haber creado ese mensaje, es el único que tiene la clave privada.
    - No repudio: por la misma razón que antes, no puede negar haber enviado el mensaje.
  - No proporciona:
    - Confidencialidad: cualquiera puede descifrarlo.
  - Es el mecanismo usado por la firma digital

5.2. Tipos de algoritmos de cifrado.

- ***Criptografía asimétrica:***

✓ Video de intypedia: ***http://www.intypedia.com/***

✓ Práctica 2.