Criptografía

Profesor: Melvin Fernández Ch.

Video 7

fidélitas

Virtual

fidélitas Virtual

Criptografía simétrica y asimétrica

Módulo: 3

Criptografía simétrica y asimétrica

Dependiendo de los pasos a aplicar para ejecutar el proceso de cifrado, los sistemas de criptografía se pueden clasificar en dos tipos básicos:

- Simétricos
- Asimétricos

Cifrado Simétrico

- En este caso, D es la función inversa de E y la clave usada en ambos casos es la misma.

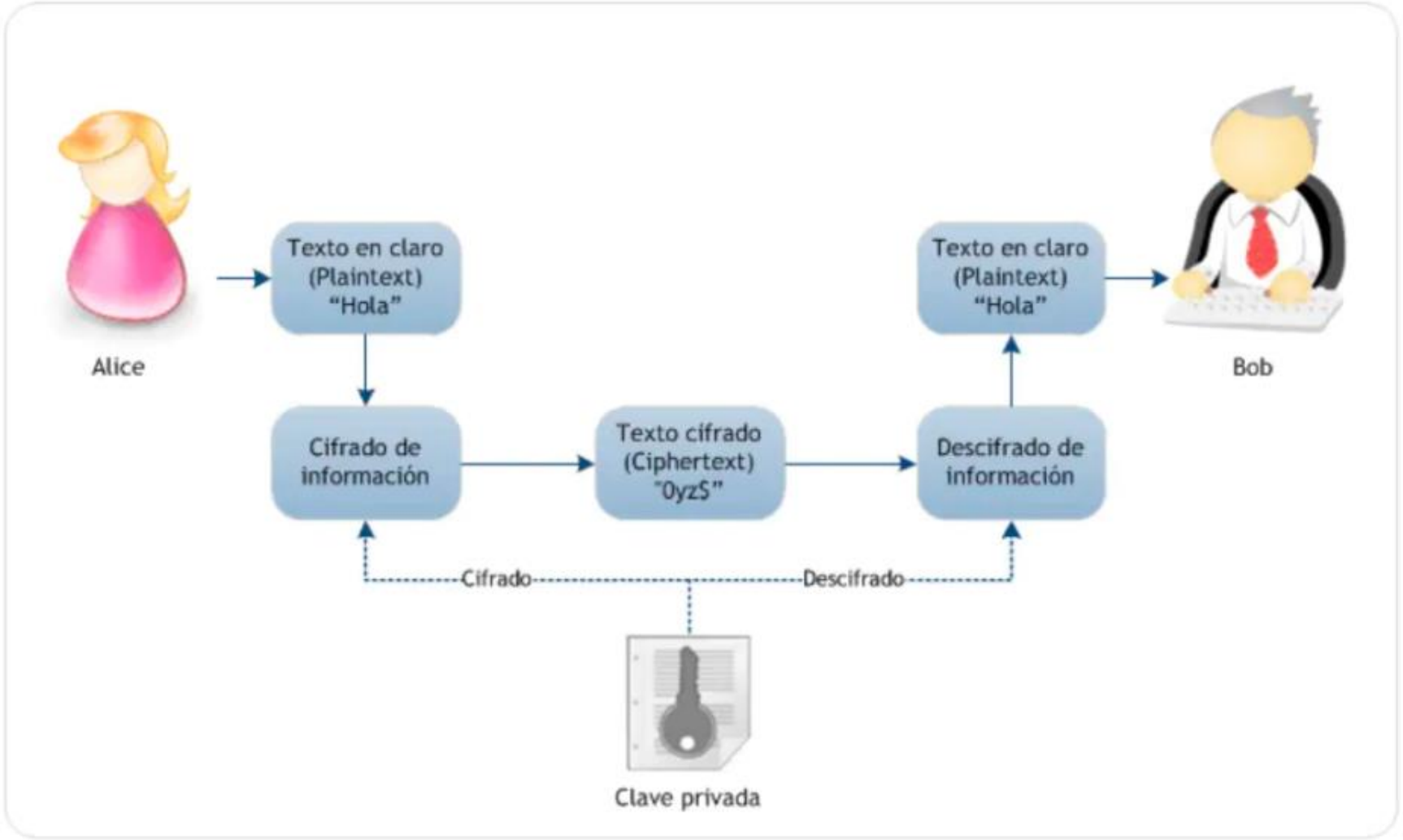
- También se denominan sistemas de clave privada, puesto que ambos utilizan la misma clave para cifrar y descifrar.

Cifrado Simétrico

- Estos métodos se caracterizan por ser muy rápidos y eficientes desde el punto de vista computacional.

- Estos métodos tienen problemas asociados con la filtración de las claves, su distribución, su debilidad criptográfica y el número creciente de claves requeridos para diferentes usuarios.

Cifrado Simétrico



Cifrado Simétrico

Algunos algoritmos de cifrado que utilizan cifrado simétrico son:

- DES (Data Encryption Estándar)
- Triple-DES
- RC2, RC4
- IDEA
- Blowfish
- AES (Advanced Encryption Standard)

Cifrado Asimétrico

- En este caso existen claves distintas pero relacionadas entre sí, una para cifrar y otra para descifrar. La función de descifrado no es exactamente inversa a la de cifrado.

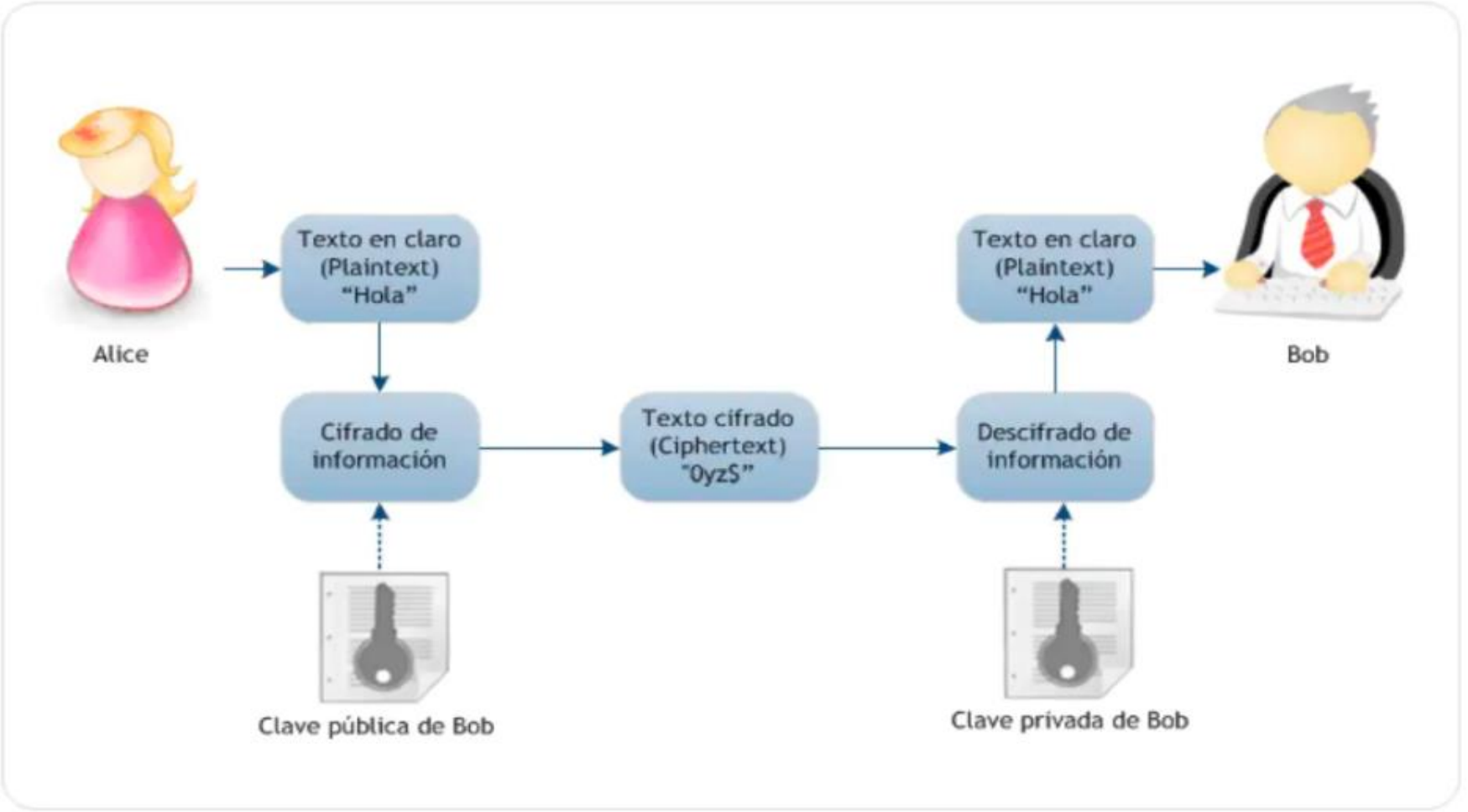
- Cada usuario posee una pareja de claves. La clave privada es utilizada para descifrar y la clave pública es utilizada para cifrar.

Cifrado Asimétrico

- La clave pública es compartida con otros usuarios para que cifren la información y la clave privada no es compartida, ya que es utilizada para descifrar.

- La asimetría permite reducir el número de claves a intercambiar entre los participantes en el proceso de cifrado y resuelve el problema del intercambio de llaves que se presenta en el cifrado simétrico.

Cifrado Asimétrico



Cifrado Asimétrico

- Una desventaja de estos algoritmos es que requieren de mayor tiempo de procesamiento por la complejidad de las operaciones matemáticas.

- Algunos algoritmos de cifrado asimétrico son:
  - Diffie y Hellman
  - RSA
  - ElGamal

Gracias

fidélitas Virtual