"CIFRADO DE DATOS"

Integrantes

Percy Saico Ccapa

Cifrado de datos

Es el proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto.

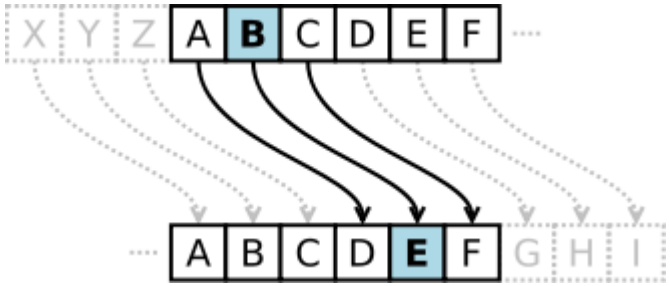
Historia del Cifrado

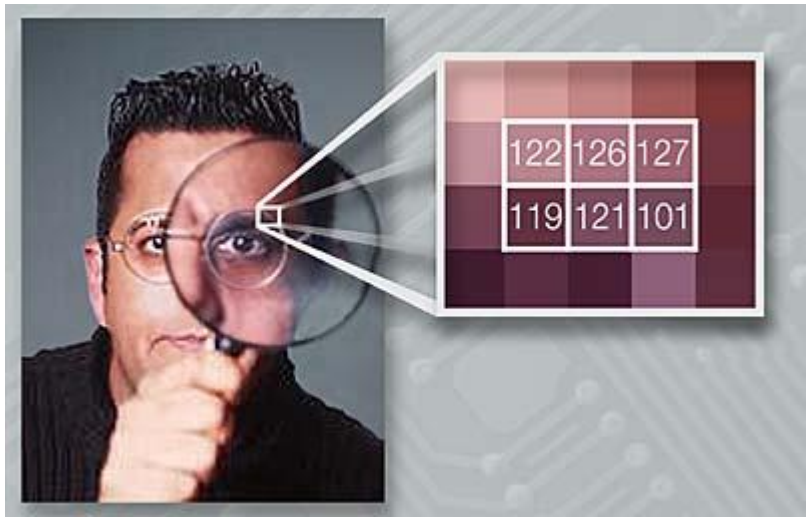
Escítala

Cifrado del César

Esteganografía

Enigma



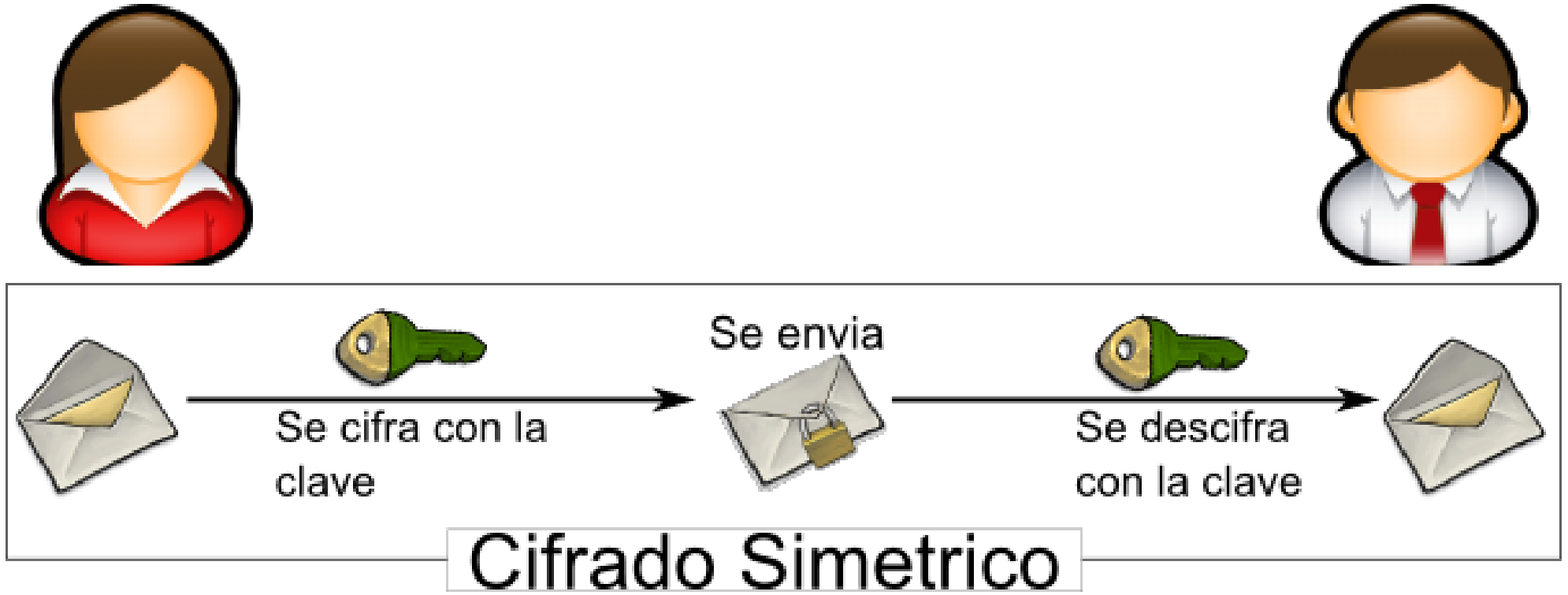


Tipos de Cifrado

- **Cifrado Simétrico**
- **Cifrado Asimétrico**
- **Cifrado Híbrido**

Cifrado Simétrico

El emisor cifra el mensaje con una clave, y esa misma clave deberá ser la utilizada para descifrarlo.



Elementos de la Encriptación Simétrica

IV (Vector de inicialización)

Esta cadena se utiliza para empezar cada proceso de encriptación.

Key (llave Publica)

Esta es la principal información para encriptar(cifrar) y desencriptar(descifrar) en los algoritmos simétricos. Toda la seguridad del sistema depende de dónde esté esta llave, cómo esté compuesta y quién tiene acceso.

Algoritmos del Cifrado Simétrico

DES (Digital Encryption Standard)

3DES (Three DES o Triple DES)

IDEA (International Data Encryption Algorithm)

AES (Advanced Encryption Standard)

El algoritmo más seguro hoy el AES, aunque 3DES también es muy seguro. Este último se utiliza cuando hay necesidad de compatibilidad. AES 128 es aproximadamente 15% más rápido que DES, y AES 256 sigue siendo más rápido que DES.

Cifrado Asimétrico

Existen dos claves, una pública y una privada, y se puede usar en dos direcciones.

Elementos del Cifrado Asimétrico

Key (llave Privada)

Llave privada (no puede conocerla nadie más), la cual se va a usar para desencriptar(Descifrar).

Key (llave Publica)

Llave pública (puede estar accesible para cualquiera), la cual se usa para encriptar(cifrar).

Algoritmos del Cifrado Asimétrico

RSA (Rivest , Shamir , Adleman)

Creado en 1978, hoy es el algoritmo de mayor uso en encriptación asimétrica. Tiene dificultades para encriptar grandes volúmenes de información, por lo que es usado por lo general en conjunto con algoritmos simétricos.

Diffie-Hellman (& Merkle)

No es precisamente un algoritmo de encriptación sino un algoritmo para generar llaves públicas y privadas en ambientes inseguros.

ECC (Elliptical Curve Cryptography)

Es un algoritmo que se utiliza poco, pero tiene importancia cuando es necesario encriptar grandes volúmenes de información.

ALGORITMOS HASH

Son algoritmos del tipo de los que se conocen como de sólo ida, ya que no es posible desencriptar lo que se ha encriptado.

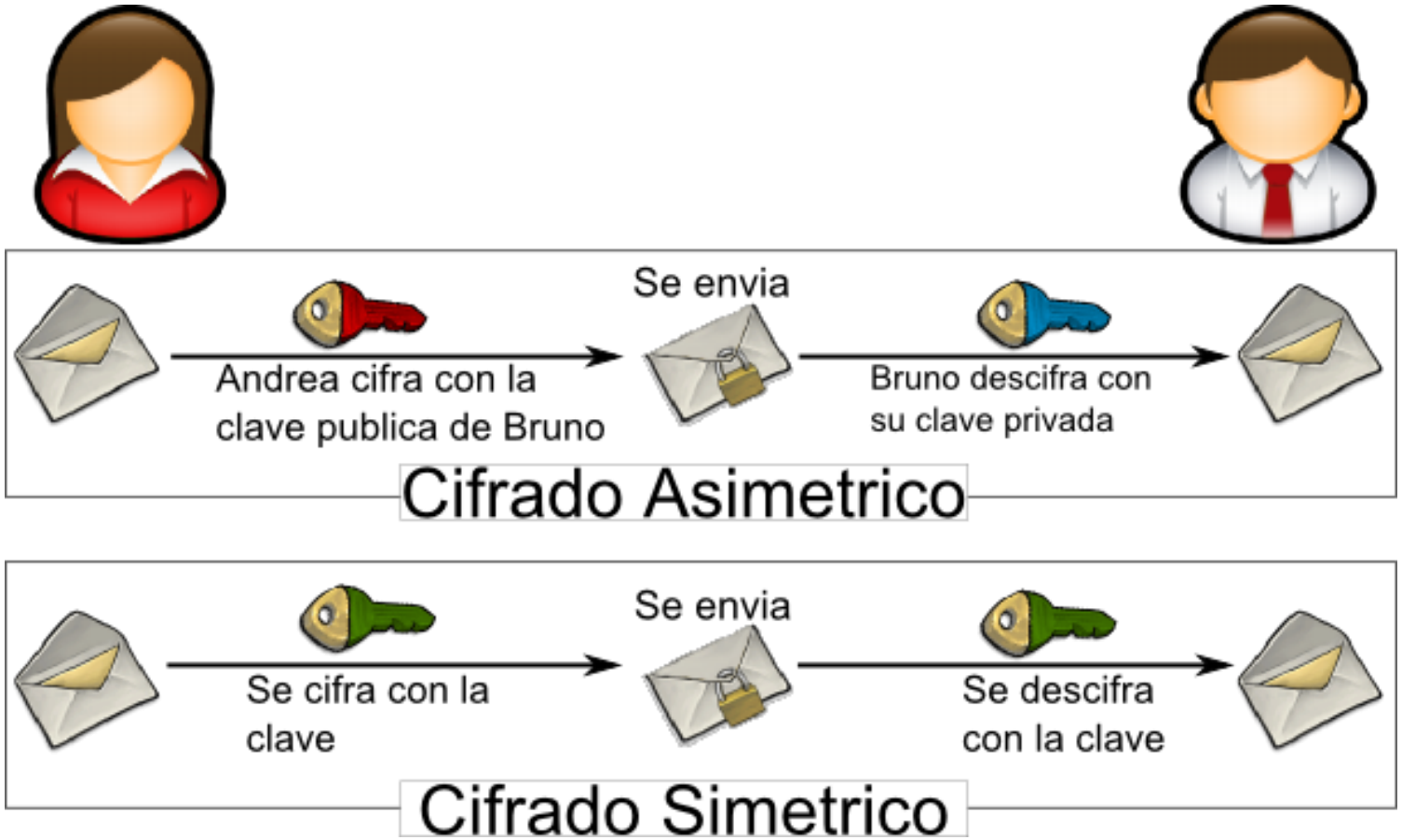
Aplicación 1: Almacenar contraseñas de un sistema.

Aplicacion 2: Validar que cierta información no se haya modificado.

Algoritmos mas conocidos: MD5, SHA-1, SHA-256, SHA-384, SHA-512

Cifrado Híbrido

Es un método criptográfico que usa tanto un cifrado simétrico como un asimétrico.



¿Que tipo de cifrado debo Elegir?

Escenario 1: Necesito almacenar información crítica que deberá poder descifrarse, y seré yo el único que haga todo el proceso. Nadie más tendrá acceso a la llave con que se encriptará y desencriptará la información.

Cifrado Simétrico

¿Que tipo de cifrado debo Elegir?

Escenario 2: Necesito que me envíen información crítica que yo desencriptaré posteriormente, pero necesito que las personas que me van a enviar información pueden encriptarla libremente, pero no desencriptarla. En este caso, se deja disponible una llave pública para que ellos encripten y yo tendré mi llave privada de encriptación en forma segura.

Cifrado Asimétrico

¿Que tipo de cifrado debo Elegir?

Escenario 3: Necesito almacenar o enviar información crítica de forma segura, pero que no requerirá ser desencriptada para su validación, o que es extremadamente importante verificar que no haya sido modificada en el camino.

Hash

Aplicaciones del Cifrado de Datos

SSL

(Secure Socket Layer), es un protocolo criptográfico que proporciona comunicaciones seguras en Internet (HTTPS,FTP,SMTP).

Firma digital

La firma digital es el método criptográfico que permite asociar la identidad de una persona o máquina a un documento como autor del mismo.

VPN Virtual Private Network (VPN), es una red con las características de una LAN, pero está extendida sobre una red pública descontrolado e inseguro como es Internet.

Cifrado de archivos

Cifrado de disco duro

Mal uso del Cifrado

- Tener un fichero cifrado en un disco duro, y que el disco duro se estropee, por lo que la información se pierda.
- La persona que sabe la clave, la olvida, o bien por deslealtad a la compañía, la filtra.
- La clave se almacena el mismo sitio que el fichero cifrado, por lo que si alguien accede al fichero cifrado también podrá acceder a la clave para descifrarlo.
- La información cifrada está corrupta o no es válida, por lo que aunque el cifrado y descifrado sean correctos, la información obtenida por el destinatario seguirá corrupta o inválida.
- Cualquier otro problema derivado de una mala gestión de la información cifrada o las claves

“NO, NO LO INTENTES. HAZLO, O NO LO HAGAS, PERO NO LO INTENTES”

MAESTRO YODA (STAR WARS)