UTT
UNIVERSIDAD TECNOLÓGICA DE TIJUANA
GOBIERNO DE BAJA CALIFORNIA

Topic:

Mecanismos de Cifrado de datos

By:

Arguelles Galvez Antonio

Group:

10B

Materia:

Creacion de Videojuegos

Teacher:

Javier Salazar Estrada

Date:

01/29/2025

Los mecanismos de cifrado de datos son técnicas que se utilizan para proteger la información, garantizando que solo las personas o sistemas autorizados puedan acceder a ella. Estos mecanismos se basan en algoritmos matemáticos para transformar datos legibles en un formato ilegible, y para revertir ese proceso cuando sea necesario. Algunos de los principales mecanismos de cifrado incluyen:

1. Cifrado simétrico

En este tipo de cifrado, tanto el emisor como el receptor utilizan la misma clave para cifrar y descifrar los datos. La principal preocupación es la seguridad de la clave, ya que debe mantenerse secreta.

- **Ejemplos**:
  - **AES (Advanced Encryption Standard)**: Algoritmo ampliamente utilizado, con claves de 128, 192 o 256 bits.
  - **DES (Data Encryption Standard)**: Un algoritmo más antiguo, menos seguro que AES.
  - **RC4**: Un algoritmo de flujo de clave secreta.

2. Cifrado asimétrico

Este tipo de cifrado usa dos claves diferentes: una pública, que se puede compartir con cualquiera, y una privada, que solo la persona propietaria de esa clave debe conocer. Los datos cifrados con la clave pública solo pueden ser descifrados con la clave privada correspondiente.

- **Ejemplos**:
  - **RSA (Rivest-Shamir-Adleman)**: Uno de los sistemas más utilizados en la criptografía asimétrica.
  - **ECC (Elliptic Curve Cryptography)**: Basado en curvas elípticas, proporciona el mismo nivel de seguridad que RSA, pero con claves más pequeñas.

3. Cifrado de clave pública (PKI)

Utiliza un par de claves: una pública y una privada. La infraestructura de clave pública (PKI) es un conjunto de políticas, tecnologías y estándares que gestionan las claves públicas y privadas, así como los certificados digitales.

4. Cifrado de hash

Aunque no es un cifrado en el sentido estricto, el hash convierte los datos en una cadena de longitud fija que representa los datos originales. Es unidireccional, lo que significa que no se puede revertir al dato original.

- **Ejemplos**:
    - **SHA (Secure Hash Algorithm)**: Varias versiones como SHA-256 y SHA-512.
    - **MD5 (Message Digest Algorithm 5)**: Un algoritmo de hash antiguo, ya obsoleto y vulnerable a ataques de colisión.

5. Cifrado de disco completo

Este tipo de cifrado cifra todo el contenido de un disco o dispositivo de almacenamiento, protegiendo todos los datos almacenados, incluidos archivos, carpetas, y el sistema operativo.

- **Ejemplos**:
    - **BitLocker**: Implementación de cifrado en sistemas Windows.
    - **FileVault**: Implementación de cifrado en sistemas macOS.

6. Cifrado homomórfico

Permite realizar operaciones sobre los datos cifrados sin necesidad de descifrarlos, lo que es útil en situaciones donde se necesitan cálculos en datos confidenciales sin exponer la información subyacente. Es una técnica emergente que aún se encuentra en desarrollo.

7. Cifrado de transporte (TLS/SSL)

Se utiliza para proteger la información durante su transmisión a través de redes, como en las conexiones HTTPS. TLS y SSL utilizan una combinación de cifrado simétrico y asimétrico para garantizar la confidencialidad e integridad de los datos durante la transferencia.

Estos mecanismos de cifrado se emplean en diferentes contextos, desde la protección de datos personales hasta la seguridad de las comunicaciones en línea. La elección del tipo de cifrado depende de las necesidades de seguridad, rendimiento y complejidad de cada sistema.