ENCRIPTADO DE DATOS

¿Qué es encriptar un dato ?

Encriptar datos es el proceso de transformar información en un formato que no se puede leer sin una clave especial o un código de acceso. Esto se hace utilizando algoritmos de cifrado que convierten los datos originales (texto plano) en un formato codificado (texto cifrado).

El objetivo principal de la encriptación es proteger la confidencialidad de la información, asegurando que solo las personas o sistemas autorizados puedan acceder y entender los datos en su forma original. Sin la clave correcta, los datos encriptados parecen aleatorios y no pueden ser descifrados fácilmente.

Primeros tipos de cifrado

Los primeros tipos de cifrado se remontan a la antigüedad, donde se utilizaban métodos simples para proteger la información, principalmente en contextos militares o políticos. Entre estos métodos se encuentra el Cifrado César, uno de los más conocidos y antiguos.

Cifrado César

El Cifrado César es un tipo de cifrado por sustitución en el que cada letra del texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Su nombre proviene de Julio César, quien supuestamente utilizaba este método para comunicarse con sus generales.

Ejemplo de Cifrado César:

Si se usa un desplazamiento de 3 posiciones:

- Texto original: `HOLA`
- Texto cifrado: `KROD`

En este caso, la `H` se desplaza 3 posiciones en el alfabeto y se convierte en `K`, la `O` se convierte en `R`, y así sucesivamente.

Características:

- Simplicidad: Es fácil de implementar, pero también fácil de romper.

Contacto: gangaritah@gmail.com

- Desplazamiento fijo: El desplazamiento es un número fijo de posiciones, lo que hace que el cifrado sea determinista y simétrico (la misma operación puede descifrar el mensaje si se conoce el desplazamiento).
- Vulnerabilidad: Debido a su simplicidad, es vulnerable a ataques de fuerza bruta y análisis de frecuencia.

Otros Primeros Tipos de Cifrado

Además del Cifrado César, otros métodos antiguos incluyen:

- Escítala Espartana: Un dispositivo utilizado por los espartanos que consistía en una varilla sobre la cual se enrollaba una tira de pergamino. El mensaje se escribía a lo largo de la varilla, y solo se podía leer correctamente si se enrollaba sobre una varilla del mismo tamaño.
- Cifrado Atbash: Un cifrado simple que invierte el alfabeto, de modo que la primera letra se reemplaza por la última, la segunda por la penúltima, y así sucesivamente.
- Cifrado de Polibio: Utilizaba una cuadrícula de letras para cifrar pares de números en lugar de letras, lo que permitía cifrar los mensajes con coordenadas numéricas.

Estos primeros métodos de cifrado son los precursores de los complejos algoritmos de encriptación utilizados en la actualidad.

Cifrado actual

Hoy en día, existen varios tipos de cifrado sofisticados que se utilizan para proteger la información en una variedad de aplicaciones, desde el almacenamiento de datos hasta la comunicación segura en internet. Estos algoritmos modernos ofrecen una mayor seguridad y son mucho más difíciles de romper que los métodos antiguos. A continuación, dos de los métodos de cifrado más usados actualmente:

Cifrado Simétrico

En el cifrado simétrico, la misma clave se utiliza tanto para cifrar como para descifrar los datos. Es rápido y eficiente, por lo que se utiliza en grandes volúmenes de datos.

- AES (Advanced Encryption Standard): Es el estándar de cifrado simétrico más utilizado en la actualidad. AES puede operar con claves de 128, 192 o 256 bits, y es ampliamente utilizado en la protección de datos confidenciales.
- DES (Data Encryption Standard): Un estándar más antiguo que utiliza una clave de 56 bits. Hoy en día se considera inseguro debido a la posibilidad de ataques de fuerza bruta.
- Triple DES (3DES): Una mejora de DES que aplica el cifrado DES tres veces a cada bloque de datos. Aunque es más seguro que DES, también es más lento y menos eficiente que AES.

Cifrado Asimétrico

El cifrado asimétrico utiliza un par de claves: una pública y una privada. La clave pública se usa para cifrar los datos, mientras que la clave privada se usa para descifrarlos. Este tipo de cifrado es fundamental para la criptografía moderna, especialmente en la seguridad de internet.

- RSA (Rivest-Shamir-Adleman): Uno de los algoritmos asimétricos más conocidos y utilizados, especialmente en la protección de datos durante la transmisión en internet. La seguridad de RSA se basa en la dificultad de factorizar grandes números primos.
- ECC (Elliptic Curve Cryptography): Un método que utiliza la matemática de las curvas elípticas para crear claves más pequeñas y eficientes, ofreciendo un nivel de seguridad comparable a RSA pero con menos recursos computacionales.

Hashing (Función de Resumen)

Aunque técnicamente no es un cifrado, el hashing es un proceso relacionado en el que los datos se convierten en una cadena fija de longitud fija (hash), que no puede revertirse para recuperar los datos originales. Se usa, entre otros, para verificar la integridad de los datos.

- **SHA-256 (Secure Hash Algorithm):** Una de las funciones hash más utilizadas en la actualidad, especialmente en la criptografía y la seguridad informática.
- **MD5 (Message Digest Algorithm 5):** Un algoritmo de hashing más antiguo que hoy en día se considera inseguro debido a sus vulnerabilidades.

Consulta

En las apps que desarrollamos:

- ¿Qué papel juega el cifrado simétrico? ¿En qué casos se usa?
- ¿Qué papel juega el cifrado asimétrico? ¿En qué casos se usa?
- ¿Qué papel juega el hashing? ¿En qué casos se usa?