Juan Emmanuel 13/10/25

Tema. Criptografía

La criptografía se define como la práctica y el estudio de técnicas para la comunicación segura en presencia de terceros. Su objetivo principal es proteger la información contra el acceso no autorizado

Por su definición, criptografía significa "texto oculto"

- Tipos de criptografía

  - Criptografía de clave simétrica
    Este tipo se basa en que ambas partes que deseen comunicarse utilizan una única clave compartida. Entre los algoritmos más conocidos están:

    * DSS (Data Encryption Standart)
    * AES (Advanced Encryption Standart

  - Criptografía de clave asimétrica
    Es fundamental en un entorno seguro en internet. Se basa en la utilización de dos claves: una pública y una privada.

Tarea 1 Hacer un programa que permita encriptar y desencriptar un archivo de texto

* RSA

La criptografía RSA es un cifrado asimetrico, que se utiliza en muchos ámbitos de la transmisión de datos en Internet por su facilidad de uso. Este consta de una clave RSA pública y otra privada, La clave pública se utiliza para el cifrado y la privada para el descifrado.

La característica más importante de este cifrado es que no hay una sola clave para descifrar un archivo, sino dos. El cifrado RSA consta de una clave pública, a la que se puede acceder libremente, y de una clave privada, que no debe ser tan accesible. El cifrado original se realiza con la clave pública RSA. En cambio, para descifrar se necesita la clave RSA privada.

Juan Emmanuel 13/10/25

*MD5
Es un algoritmo de reducción criptográfico de 128 bits utilizado para autentificar mensajes y verificar el contenido y las firmas digitales. El MD5 se basa en una función hash que verifica que un archivo enviado coincide con el recibido, evitando que haya sufrido alteraciones en su envío.

MD5 cifra archivos enteros a través de un algoritmo de hashing matemática para generar una firma. Este algoritmo convierte los datos en una cadena de 32 caracteres. Se utiliza una complejo fórmula matemática para crear un hash. convierte los datos en bloques de tamaños específicos y los manipula varias veces. Mientras esto ocurre, el algoritmo añade un valor único en el cálculo y convierte el resultado en una pequeña firma o hash. La misma entrada genera la misma salida, también conocida como la suma MD5, el hash o la suma de verificación

*Base 64
Es un algoritmo de codificación que permite transformar cualquier caracter de cualquier idioma en un alfabeto que consta de letras, dígitos y signos latinos. Con esto se puede convertir caracteres especiales en una secuencia legible que se puede guardar y/o transferir en cualquier otro lado. Es utilizado para transmitir datos binarios por medio de transmisiones que tratan sólo con texto, como para enviar imagenes y archivos adjuntos por correo electronico.

Su alfabeto consta de 64 caracteres que dieron lugar a su nombre.
Este algoritmo encripta y desencripta