¿Qué quiere decir Criptografía?

Datos Sincronizados

Escritura Oculta

Datos enmarcados

Lectura de Datos

Seleccione cuales no pertenecen a una definición de Estenografía

Es una técnica encargada de hacer la información invisible.

Trata de mantener la información clasificada oculta para todo público.

Es utilizada en forma de seguridad para proteger la privacidad de un mensaje.

Es la técnica de proteger la privacidad del mensaje al transmitirlo por un medio.

Implica la modificación visible de archivos multimedia para esconder información confidencial.

Una según corresponda los conceptos de Criptografía

Criptografía Asimétrica

Esta técnica usa dos claves distintas para el cifrado y descifrado de un texto.

Criptografía Simétrica

Esta técnica utiliza la misma clave tanto para el cifrado como para el descifrado de un mensaje.

Criptografía Hash

Estas son claves únicas que se generan con un algoritmo.

Criptografía de Ofuscación

Con esta técnica no se consigue evitar ataques, sino más bien retrasarlos; pero puede ser útil en algunos contextos.

Complete la frase:

Tradicionalmente los **datos** se tenían que descifrar antes de poder utilizarlos en un **cálculo**.

Seleccione verdadero o falso:

Hay 2 elementos importantes de la mecánica cuántica de los que depende la criptografía cuántica: el principio de **incertidumbre de Heisenberg** y el principio de **acción y reacción**

FALSO

verdadero

Hay 2 elementos importantes de la mecánica cuántica de los que depende la criptografía cuántica: el principio de **incertidumbre de Heisenberg** y el principio de **polarización de fotones** .

PRESENTACIÓN DE CIFRADO SIMÉTRICO / CRITOGRAFÍA SIMÉTRICA

Como ya vimos la criptografía se basa en el ocultamiento de la información, en este caso una de sus ramas de estudio que es el cifrado simétrico el cual también se lo conoce como cifrado de **código único** con lo cual es mensaje es íntegro y auténtico.

Donde el emisor y el receptor deben tener una clave compartida para poder entender el mensaje.

Radica en que tan fuerte sea la clave secreta para mantener la **integridad de la información.**

Velocidad y eficiencia:

- Operaciones mas simples dado que es UNO a Uno
- Menos sobrecarga computacional
- Procesamiento en bloque
- Algoritmos optimizados como: AES

CLASIFICACIÓN

1. **Cifrado de Flujo**
   Cifran el texto plano de manera continua bit a bit, byte a byte.
   Utilizando una secuencia de claves internamente.
   Ejemplos: Algoritmos RC4 y Salsa20
   RC4: Inicialmente fue diseñado para redes inalámbricas.
   Genera una secuencia pseudo aleatoria de bytes que se combina con el texto plano para producir el texto cifrado
   Salsa20: Conocido por su velocidad, simplicidad y resistencia a ataques. Genera una clave pseudoaleatoria con un cifrado de bloque de 32 bits a manera de bucle.

   Entre RC4 y Salsa20 ambas son rápidas, pero RC4 es mas obsoleta y se usa mejor la Salsa20 para un mejor manejo de la seguridad.

2. **Cifrado de Bloque**
   Divide el texto plano en bloques fijos y los cifra por separado, usando la misma clave.
   Ejemplos: Algoritmos AES (Estándar de Cifrado Avanzado), 3DES (Tripe Des)
   AES: Opera un bloque de datos de 128 bits y claves de 128,192 o 256 bits, se genera el cifrado usando combinación de sustituciones y permutaciones.
   3DES: Es una mejora del DES. Opera el bloque de 64 bits con claves de 56 bits. Aplica el **cifrado-descifrado y -cifrado nuevamente**, aumentando así la seguridad de los datos.

   La más usada es la AES por ser más vigente SIENDO MAS SEGURA Y EFICIENTE y La menos usada la 3DES.

   ### EJEMPLOS DE APLICACIONES DE ESTAS SUB CATEGORIAS

   1. RC4:
   - WEP (Wired Equivalent Privacy): Este protocolo de seguridad fue utilizado en redes inalámbricas WiFi antes de ser reemplazado por WPA y WPA2 debido a sus debilidades de seguridad. Aunque ya no es ampliamente utilizado, algunos dispositivos y aplicaciones antiguas aún pueden implementarlo.

   2. Salsa20:
   - OpenSSH: Salsa20 es uno de los algoritmos de cifrado simétrico disponibles en OpenSSH, una herramienta utilizada para conectarse y gestionar sistemas de forma segura a través del protocolo SSH.

   3. AES (Advanced Encryption Standard):

- WhatsApp: Utiliza AES para cifrar las conversaciones de extremo a extremo, lo que significa que solo el remitente y el destinatario pueden leer los mensajes.
- BitLocker: Esta herramienta de cifrado de disco duro integrada en Windows utiliza AES para proteger los datos almacenados en el disco.

4**. 3DES (Triple Data Encryption Standard):**
- OpenVPN: Es un software de código abierto que implementa una red privada virtual (VPN) utilizando 3DES, entre otros algoritmos, para cifrar la comunicación entre dispositivos.
- Hardware de seguridad: Algunos dispositivos de seguridad de hardware, como tarjetas inteligentes y tokens USB, utilizan 3DES para proteger la información confidencial almacenada en ellos.

EJEMPLOS GENERALES

Cifrado César: Usado por Julio Cesar en la Antigua Roma

Desplazar cada letra del alfabeto por un número fijo de posiciones.

Cifrado Vigenere: Usada en el renacimiento

Consistía en utilizar una palabra clave para cifrar el texto desplazando la letra según lo acordado.

Encriptación de correo: Usado en correo electrónico con el protocolo OpenPGP. Cuando el emisor envía el mensaje utiliza una clave pública del destinatario para cifrar una clave simétrica.

Encriptación Disco Duro: Puede ser todo el disco o una partición mediante AES

DATOS DE INTERES:

Un cifrado, en su forma más básica, comprende tres elementos principales:

1. Algoritmo de cifrado: Es el conjunto de reglas o procedimientos que se utilizan para transformar el texto original en texto cifrado. El algoritmo puede variar según el método de cifrado utilizado, como el cifrado César, el cifrado de sustitución, el cifrado de Vigenère, etc.

2.Clave: Es un parámetro necesario para el algoritmo de cifrado. La clave determina cómo se lleva a cabo la transformación del texto original en texto cifrado y, en el caso de los cifrados simétricos, también se utiliza para descifrar el texto cifrado y restaurarlo a su forma original. La seguridad del cifrado suele depender en gran medida de la complejidad y seguridad de la clave utilizada.

3. Texto plano (o mensaje original): Es el texto que se desea cifrar. Puede ser cualquier forma de datos, como texto, números, o cualquier tipo de archivo binario.

Además de estos elementos básicos, en algunos cifrados pueden intervenir otros elementos como vectores de inicialización, tablas de sustitución, entre otros, dependiendo de la complejidad y el tipo de cifrado utilizado.

El término "polialfabético" se refiere a un método de cifrado que utiliza más de un alfabeto o tabla de sustitución para cifrar el texto.