NOMNRE DEL ALUMNO: EDDI DAVID AGULAR MARTINEZ

NOMBRE DEL PROFESOR: JORGE ALBERTO HERNANDEZ PEREZ

MARERIA: REDES DE COMPUTADORAS III

TIPO DE TRABAJO: SUPERNOTA

LICENCIATURA: INGENIERIA EN SISTEMAS COMPUTACIONALES

CUATRIMESTRE: 7

LA CRIPTOGRAFIA

Introducción a la criptografía (Mencionar tres datos históricos)

herramienta muy útil cuando se desea tener seguridad informática;

Los primeros mensajes cifrados datan del siglo V a.C

La era de la criptografía moderna comienza realmente con Claude Shannon, que podría decirse que es el padre de la criptografía matemática.

El primer punto de inflexión en el desarrollo de los sistemas criptográficos se produjo durante la Segunda Guerra Mundial, con el uso por parte del ejército nazi de la máquina de cifrado Enigma.

Dos principios criptográficos fundamentales.

Criptografía de clave publica

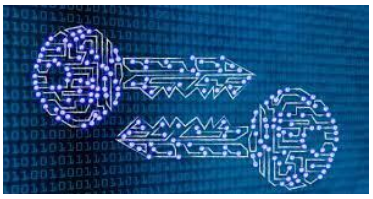
Este punto lo analizaremos como más detalle en el tema. Básicamente consiste en utilizar dos claves, una publica y otra privada, para cifrar los mensajes de la comunicación.

criptoanálisis

El objetivo del criptoanálisis es encontrar alguna debilidad o inseguridad en un esquema de cifrado. La mayoría de los sistemas de cifrado, se pueden romper con un esfuerzo computacional suficiente por ataques de fuerza bruta, pero la cantidad de esfuerzo necesario puede ser exponencial dependiendo del tamaño de la clave en comparación con el esfuerzo necesario para hacer el uso del cifrado.

Seguridad

La app de mensajería más utilizada, WhatsApp, fue pionera en la implantación del cifrado de extremo a extremo al incorporarlo a su política de privacidad en 2016. El cifrado garantiza que sólo el emisor y el receptor puedan leer o escuchar lo que se envía, de modo que ni siquiera el personal de WhatsApp tiene acceso a los datos.



Cifrado de clave simétrica

La criptografía de clave simétrica es un término utilizado para los algoritmos criptográficos que utilizan la misma clave para el cifrado y el descifrado. La clave se suele llamar "clave simétrica" o "clave secreta".

Los algoritmos de clave simétrica son seguros y altamente eficientes cuando se usan de manera adecuada, de modo que pueden usarse para cifrar grandes cantidades de datos sin tener un efecto negativo en el rendimiento.

Cifrado de clave asimétrica

La criptografía asimétrica, también conocida como criptografía de clave pública o criptografía de dos claves, es un sistema criptográfico que se caracteriza por utilizar dos claves, una clave pública y otra privada, para el envío de mensajes o datos informáticos.

Cifrado hash

Una función criptográfica hash- usualmente conocida como "hash"- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

FUNETES DE INFORMACION

- https://plataformaeducativauds.com.mx/assets/docs/libro/ISC/876e6c2bdd20ba64820e9d099bd430cf-LC-ISC701%20REDES%20DE%20COMPUTADORAS%20III.pdf