UNIVERSIDAD DEL SURESTE: DE LA FRONTERA COMALAPA.

DOCENTE: Icel Bernardo Lepe Arriaga.

ASIGNATURA: Redes de computadoras “III”.

ALUMNO: Ramiro Gerardo Resendíz Valdéz.

CUATRIMESTRE: Séptimo (7mo).

CARRERA: Ingeniería en sistemas computacionales.

GRUPO: ISC13SDC0220-A.

UNIDAD: Primera (1ra).

TRABAJO: Mapa conceptual de la unidad uno de la antología.

FECHA DE ENTREGA: 25/Septiembre/2022


Criptografía.
Introducción a la criptografía.
Criptografía es la ciencia encargada de transformar la información de manera tal que ésta quede descubierta y sea incompresible para todo aquel que no tenga la autorización correspondiente para acceder a ella.
En el siglo V a.C. durante la guerra entre Atenas y Esparta, se encuentra el primer registro formal del uso de escritura secreta, en el 400 a.C.
La criptografía, en términos sencillos es la ciencia que se basa en la escritura de códigos y cifrados para proteger las comunicaciones, es uno de los elementos más importantes que hacen posible la existencia de criptomonedas modernas y blockchains.
Dos principios criptográficos fundamentales.
Aunque la criptografía es muy variada existen dos principios fundamentales que sostienen la criptografía y que es importante entender.
Si una persona lee un mensaje en el que faltan algunas letras, normalmente puede reconstruirlo.
El segundo principio criptográfico es el de actualización el cual implica que se deben tomar medidas para asegurar que cada mensaje recibido se verifique a fin de saber siesta actualizado.
Cifrados por sustitución.
El cifrado César es uno de los primeros métodos de cifrado conocidos históricamente. Julio César lo usó para enviar órdenes a sus generales en los campos de batalla.
Consistía en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas tres posiciones a la derecha.
Una sustitución mono alfabeto como la del cifrado César puede expresarse mediante una transformación congruente lineal (también conocida criptográficamente como transformación afín).
Aparentemente es un cifrado muy débil y poco seguro, pero en la época de Julio César no era de conocimiento general la idea de ocultar el significado de un texto mediante cifrado.
Rellenos de una sola vez.
La construcción de un cifrado inviolable es bastante sencilla. La técnica se conoce desde hace décadas y consiste en escoger una cadena de bits al azar como clave.
El texto cifrado resultante no puede descifrarse porque cada texto normal posible es un candidato igualmente probable. El texto cifrado no proporciona al criptoanalista ninguna información en absoluto.
La criptografía clásica se basa en algoritmos sencillos y claves muy largas para la seguridad. Las técnicas criptográficas clásicas son básicamente dos, el cifrado por sustitución y el cifrado por trasposición.