UNIVERSIDAD DEL SURESTE DE LA FRONTERA COMALAPA

ASIGNATURA: Redes de Computadoras III

DOCENTE: Icel Bernardo Lepe Arriaga

ALUMNO: Josué Roberto Pérez López

CUATRIMESTRE: Séptimo

GRUPO: A

CARRERA: Ingeniería en sistemas computacionales.

PARCIAL: Primero

TRABAJO: Mapa Conceptual Unidad I

FECHA: 24 de Septiembre de 2022.

CRIPTOGRAFIA

¿Qué es?

Se refiere al arte de escribir mensajes en clave secreta o en forma enigmática, así, en nuestros días, 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

CIFRADO POR SUSTITUCIÓN

El cifrado César es uno de los primeros métodos de cifrado conocidos históricamente. Consiste en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas tres posiciones a la derecha.

- Cifrados por sustitución mono alfabeto
- Criptoanálisis de los Métodos de Cifrado Monoalfabéticos
- Cifrados de sustitución poli alfabeto
- Cifrado de Vigenère

CIFRADO POR TRASPOSICIÓN

El método de cifrado por transposición consiste en reordenar datos para cifrarlos a fin de hacerlos ininteligibles. Esto puede significar, por ejemplo, reordenar los datos geométricamente para hacerlos visualmente inutilizables.

- Cifrado por transposición columnar
- Cifrado por transposición

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. Luego se convierte el texto normal en una cadena de bits, por ejemplo, usando su representación ASCII. Por último, se calcula el or exclusivo (XOR) y cuya tabla de valores lógicos puede verse en la siguiente figura, de estas dos cadenas, bit por bit.

Sin embargo, este método tiene varias desventajas prácticas.
En primer lugar, la clave no puede memorizarse, por lo que tanto el transmisor
como el receptor deben llevar una copia por escrito consigo. Además, la
cantidad total de datos que pueden transmitirse está limitada a la cantidad de
clave disponible. Otro problema es la sensibilidad del método a la pérdida o
inserción de caracteres. Si el transmisor y el receptor pierden la sincronía,
todos los datos a partir de ahí aparecerán alterados.

DOS PRINCIPIOS CRIPTOGRAFICOS FUNDAMENTALES

El primer principio es que todos los mensajes cifrados deben contener redundancia, es decir, información no necesaria para entender el mensaje.
Definiremos redundancia como cierta repetición de la información contenida en un mensaje, que permite, a pesar de la pérdida de una parte de este, reconstruir su contenido.

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. Esto permite evitar que posibles intrusos activos reproduzcan mensajes antiguos. Una de las medidas es incluir en cada mensaje una marca de tiempo válida por ejemplo durante 10 segundos, para compararlo con los mensajes nuevos que lleguen y filtrar los duplicados. Los mensajes con una antigüedad mayor a10 segundos pueden descartarse.