UNIVERSIDAD DEL SURESTE

Materia:

Redes de Computadoras

Alumno(a):

Jirem Madali Jiménez Trejo

7° cuatrimestre

Docente:

Ing. Eduardo Genner Escalante Cruz

REDES DE COMPUTADORAS

Principio de funcionamiento

Se trata de un sistema de cifrado simétrico por bloques de 64 bits, de los que 8 bits (un byte) se utilizan como control de paridad (para la verificación de la integración de la clave.

DES (DATA ENCRYPTION STANDARD): El estándar de encriptación de datos, es un esquema de encriptación simétrico desarrollador en 1997 por el departamento de comercio y la oficina nacional de estándares de EEUU en colaboración con la empresa IBM

CRIPTOLOGIA: Del griego Kriptós, criptos- ocultar y graphé, grafos- escribir, (escritura oculta).

CIFRADO CESAR

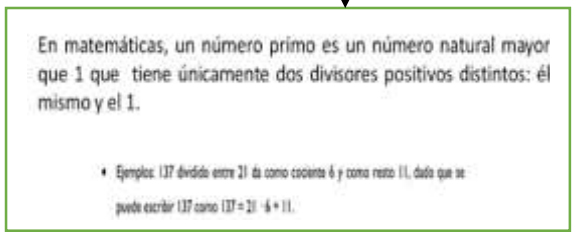
Cifrados por sustitución: se trata de cambiar la letra correspondiente por otra en un sistema ordenado siguiendo un patrón.

Permutación: es la variación del orden o posición de los elementos de un conjunto ordenado o una tupla.

Características: ofrecer un alto nivel de seguridad relacionado con una pequeña clave utilizada para cifrado o descifrado, ser comprensible, no depender de la confidencialidad del algoritmo, ser adaptable y económico, ser eficaz y exportable.

TDES: Este método de cifrado es inmune al ataque por encuentro a medio camino, doblando la longitud efectiva de la clave (112 bits), pero en cambio es preciso triplicar el número de operaciones de cifrado, haciendo este métodos de cifrado muchísimo más seguro que el DES.

RSA: Método de encriptado de datos, es uno de los más usados hoy día para la transmisión segura de datos a través de canales inseguros.



SEGURIDAD EN REDES:

Errores en seguridad:

1. Claves cortas
2. Claves sin números o símbolos
3. Usar datos personales
4. Usar fechas de nacimiento, dirección o número de teléfono
5. Compartir información con el maestro.

Recomendaciones de seguridad:

Cambia tu contraseña.

No uses la misma clave, al menos cambia un número.

Usa número, mayúscula y símbolo.

RECUERDA todo lo que pasa en la red (es inseguro) **TODO**.

- Usa recursos con seguridad
- Protege tu información
- Piensa antes de enviar

CLAVES PÚBLICAS Y PRIVADAS

Un firewall, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso.

El robo de identidad (Identity theft o "ID theft") se produce cuando una persona adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la intención de efectuar o vincularlo con algún fraude u otro delito.

Tor Browser es un navegador gratuito de código abierto configurado para funcionar en la red Tor, en la que tus páginas pasan encriptado por varios servidores antes de salir a internet, ofuscando su origen para mejorar tu privacidad y sirve para evadir los bloqueos en internet.

Https es "Hyper Text Transfer Protocol" con una 'S' añadida al final, que hace referencia a "Secure Sockets Layer" otro importante protocolo desarrollado para realizar transferencias de forma segura en Internet usando nuestro navegador.

Un proxy es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos.

VPN: Una red privada virtual (RPV) (en inglés, Virtual Private Network, VPN) es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como

SSL: Se trata de protocolos criptográficos que proporcionan privacidad e integridad en la comunicación entre dos puntos en una red de comunicación. Esto garantiza que la información transmitida por dicha red no pueda ser interceptada ni modificada por elementos no autorizados, garantizando de esta forma que sólo los emisores y los receptores legítimos sean los que tengan acceso a la comunicación de manera íntegra.

ATAQUES DE DENEGACION DE SERVICIO: También llamado ataque DDoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.