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 (2da).

TRABAJO: Cuadro de la unidad dos de la antología.

FECHA DE ENTREGA: 16/Octubre/2022

UNIDAD II
Algoritmos de claves simetricas.

DES-el estándar de encriptación de datos.

A finales de 1974, IBM propuso "Lucifer", que gracias a la NSA (National Standard Agency, en castellano: Agencia Nacional de Seguridad) fue modificado el 23 de noviembre de 1976, convirtiéndose en DES (Data Encryption Standard, en castellano: Estándar de Cifrado de Datos).

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 integridad de la clave).

El algoritmo se encarga de realizar combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave, asegurándose al mismo tiempo de que las operaciones puedan realizarse en ambas direcciones (para el

Una vez que la permutación inicial se completó, el bloque de 64 bits se divide en dos bloques de 32 bits denominados I y D respectivamente (para izquierda y derecha, siendo la anotación en anglo-sajón L y R por Left y Right).

AES-el estándar de encriptación avanzada.

AES significa Advanced Encryption Standard. Aunque sus raíces se remontan a 1997, actualmente sigue siendo el único algoritmo en la lista del National Institute of Standards and Technology (NIST) para proteger datos clasificados.

AES es lo que se conoce como un cifrado simétrico por bloques, lo que significa que cifra y descifra los datos en bloques de 128 bits cada uno.

AES-256 – la versión clave de 256 bits de AES – es el estándar de cifrado utilizado por Le VPN. Es la forma más avanzada del cifrado y consiste en 14 rondas de sustitución, transposición y mezcla para un nivel de seguridad excepcionalmente alto.

AES-256 también tiene la ventaja de ser extremadamente rápido. Cuando navegas por la web con una VPN que utiliza el cifrado AES-256 en sus servidores, no experimentarás ninguna disminución en el rendimiento en comparación con otro protocolo de seguridad.

UNIDAD II
Algoritmos de claves simetricas.

## Modos de cifrado.

Los algoritmos de cifrado por bloque pueden ser ejecutados de diferentes modos.

Mostramos ahora los modos más extendidos. Supondremos que el alfabeto de nuestro bloque a cifrar es Σ y que la longitud del bloque es.

En este modo, el texto plano se descompone en bloques de longitud. Si es necesario, al texto plano se le añade un suplemento para conseguir que su longitud sea divisible por, en este modo, cada bloque de longitud es cifrado de forma independiente al resto de bloque

Cuando se usa este modo, a iguales bloques de texto plano se obtienen iguales bloques de texto cifrado, es así posible reconocer algunos patrones del texto plano en el texto cifrado. Eso facilita un ataque estadístico.

Otra vulnerabilidad de este modo de cifra es que un atacante puede sustituir algunos bloques del texto cifrado con otros bloques cifrados que hayan sido cifrados con la misma clave, esta manipulación es difícil de detectar en el receptor.

## Otros cifrados.

Cada letra (o carácter) se intercambia por otra del mensaje, reordenando de algún modo las letras, pero no disfrazándolas. Para este tipo de cifrado se usan multitud de métodos, como colocar las letras en una matriz de una manera y sacarlas de otra manera diferente.

Según el principio de Kerkhoff todos los algoritmos de cifrados y descifrados deben ser públicos y conocidos por todos, lo único secreto es la clave del algoritmo, esta clave se convierte en la piedra angular del algoritmo.

Basándose en este principio, el cifrado perfecto (el cifrado Vernam) debe ser público con su clave en secreto y ésta debe tener la misma longitud del mensaje, ser generada aleatoriamente y solamente puede ser usada una sola vez.

Como se puede observar este método sería perfecto de no ser porque cada clave generada aleatoriamente debería ser generada también aleatoriamente e idéntica a la del emisor, por el receptor del mensaje, algo que en principio es muy difícil.

UNIDAD II
Algoritmos de claves simetricas.

Criptoanálisis.

como el estudio de los métodos para obtener sentido a un mensaje cifrado, también es conocido como la ciencia opuesta a la Criptografía. Estos métodos se traducen típicamente en conseguir la clave secreta con la cuál fue cifrado el mensaje.

Es la ciencia opuesta a la criptografía quizás no es muy afortunado hablar de ciencias opuestas, sino más bien de ciencias complementarias, ya que, si ésta trata principalmente de crear y analizar criptosistemas seguros.

Si el atacante conoce el algoritmo de cifrado y sólo tiene acceso al criptograma, se plantea un ataque sólo al criptograma; un caso más favorable para el criptoanalista se produce cuando el ataque cumple todas las condiciones del peor caso; en este caso, el criptoanálisis se denomina de texto en claro conocido.

El algoritmo de cifrado, para ser considerado seguro, ha de soportar todos estos ataques y otros no citados; sin embargo, en la criptografía, como en cualquier aspecto de la seguridad, informática o no, no debemos olvidar un factor muy importante: las personas.