UNIVERSIDAD DEL SURESTE

SAN CRISTOBAL DE LAS CASAS CHIAPAS

MATERIA: REDES DE COMPUTADORA

TRABAJO: MAPA CONCEPTUAL

NOMBRE DEL ALUMNO: BALDOMERO SANTIZ GOMEZ

SEMESTRE: 7MO. CUATRIMESTRE

GRUPO: “A”

CARRERA: ING. EN SISTEMAS COMPUTACIONALES

CATEDRÁTICO: MCC. EDUARDO GENNER ESCALANTE

FECHA DE ENTREGA: 22/10/2020

CIFRADO DE DATOS

En el mundo de la **informática**, el **cifrado** es la conversión de **datos** de un formato legible a un formato codificado, que solo se pueden leer o procesar después de haberlos descifrado.

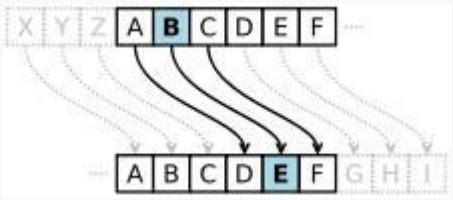
Los dos **tipos de cifrados** más importantes son: el simétrico y el asimétrico. Criptografía Simétrica: es aquella que utiliza la misma clave para **cifrar** y descifrar el mensaje y que previamente deben conocer el emisor y el receptor. Criptografía Asimétrica: es aquella que utiliza dos claves.

El algoritmo AES (Advanced Encryption Standard) es uno de los algoritmos **más seguros** que existen hoy en día.

El algoritmo 3DES (Triple Data Encryption Standard), se basa en el algoritmo DES, que aplica una serie de operaciones básicas para convertir un texto en otro cifrado, empleando una clave criptográfica.

CIFRADO DE CESAR

Cifrado César



El cifrado César mueve cada letra un determinado número de espacios en el alfabeto. En este ejemplo se usa un desplazamiento de tres espacios, así que una B en el texto original se convierte en una E en el texto codificado.

En criptografía, el cifrado César, también conocido como cifrado por desplazamiento, código de César o desplazamiento de César, es una de las técnicas decodificación más simples y más usadas.

Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etc. Este método debe su nombre, según Suetonio, a Julio César, que lo usaba para comunicarse con sus generales.

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.

Alfabeto en claro:	A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z
Alfabeto cifrado:	D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C

RSA

En criptografía, **RSA** (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1979. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

El **sistema criptográfico con clave pública RSA** es un algoritmo asimétrico cifrador de **bloques**, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario..

Una clave es un número de gran tamaño, que una persona puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits o bytes.

Los mensajes enviados usando el **algoritmo** RSA se representan mediante números y el funcionamiento se basa en el producto de dos **números primos** grandes (mayores que 10^{100}) elegidos al azar para conformar la clave de descifrado.

DES

DES (Data Encryption Standard) es un esquema de encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EEUU en colaboración con la empresa IBM, que se creó con objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de ordenadores.

Estaba basado en la aplicación de todas las teorías criptográficas existentes hasta el momento, y fue sometido a las leyes de USA.

Posteriormente se sacó una versión de DES implementada por hardware, que entró a formar parte de los estándares de la ISO con el nombre de DEA.

Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones.

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

Como la clave efectiva es de 56 bits, son posible un total de 2 elevado a 56 = 72.057.594.037.927.936 claves posibles, es decir, unos 72.000 billones de claves, por lo que la ruptura del sistema por fuerza bruta o diccionario es sumamente improbable, aunque no imposible si se dispone de suerte y una gran potencia de cálculo.

LLAVES SIMÉTRICAS

El mecanismo de cifrado basado en **claves simétricas** consiste en que el emisor y el destinatario tienen que compartir una misma clave para cifrar y descifrar la información

Los sistemas de cifrado **simétrico** son aquellos que utilizan la misma clave para cifrar y descrifrar un documento. El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave.

LLAVES ASIMETRICOS

Algoritmo asimétrico. Es un **algoritmo** que modifica los datos de un documento con el objeto de alcanzar algunas características de seguridad como autenticación, integridad y confidencialidad. También conocidos como **algoritmos** de llave pública