



NOMBRE DEL ALUMNO: MARLONG URIEL RAMOS
DOMINGUEZ

NOMBRE DEL PROFESOR: JORGE ALBERTO
HERNANDEZ PEREZ

CUATRIMESTRE:7

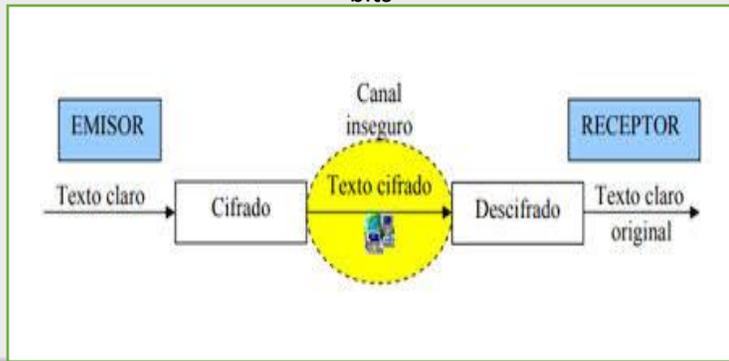
INGENIERIA EN SISTEMAS COMPUTACIONALES
REDES DE COMPUTADORAS 3

Una red de ordenadores se refiere a dispositivos de computación interconectados que pueden intercambiar datos y compartir recursos entre sí. Los dispositivos de la red utilizan un sistema de reglas, llamados protocolos de comunicaciones, para transmitir información a través de tecnologías físicas o inalámbricas.

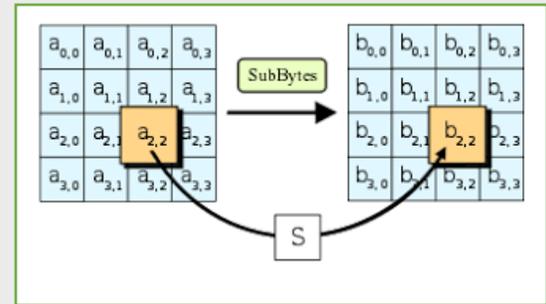
Respondamos algunas preguntas frecuentes comunes sobre la red de ordenadores.

Los nodos y los enlaces son los componentes básicos de las redes de ordenadores. Un nodo de red puede ser un equipo de comunicación de datos (DCE), como un módem, un concentrador o un conmutador, o un equipo terminal de datos (DTE), como dos o más ordenadores e impresoras. Un enlace se refiere a los medios de transmisión que conectan dos nodos. Los enlaces pueden ser físicos, como cables o fibras ópticas, o espacio libre utilizado por redes inalámbricas.

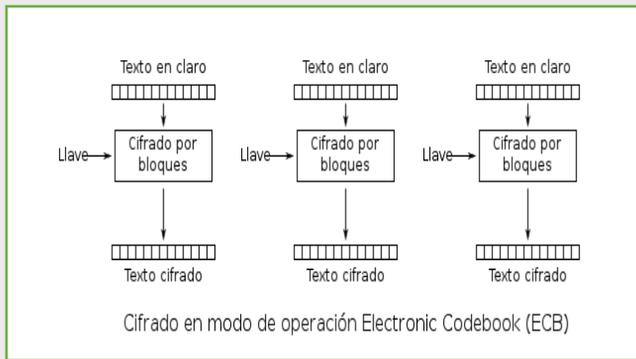
DES-EL ESTANDAR DE ENCRIPCIÓN DE DATOS; Estándares de cifrado de datos (DES): DE es un algoritmo de cifrado de bloques de cifrado bajo nivel que convierte texto sin formato en bloques de 64 bits y los convierte en texto cifrado utilizando claves de 48 bits



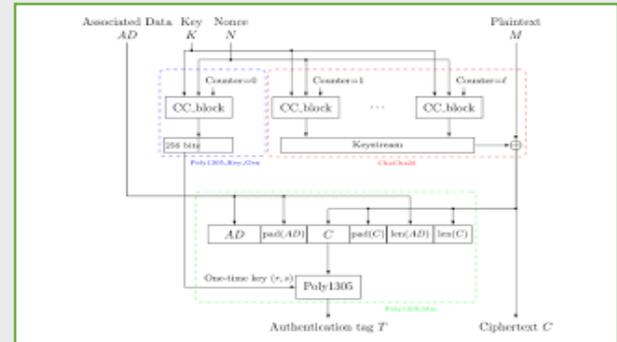
AES-EL ESTADO DE ENCRIPCIÓN AVANZADA: es un estándar de cifrado adoptado por el gobierno de los Estados. El estándar consiste en tres cifras de bloques, AES-128, AES-192 y AES-256, adoptados de una gran colección originalmente publicada como Rijndael.



MODOS DE CIFRADO: un modo de operación es un algoritmo que utiliza un cifrador por bloques para proveer seguridad a la información, como confidencialidad y autenticidad. Un cifrador por bloques en sí mismo sólo es adecuado para la transformación criptográfica segura de un grupo de bits de longitud fija llamado bloque



CHACHA20: es un algoritmo de cifrado, que soporta claves de 128 y 256 bits y de alta velocidad también creado por Bernstein en 2008. Tiene características similares a Salsa20, pero con un función primitiva de 12 o 20 rondas distintas.



CIFRADO TWOFISH: Twofish es un método de criptografía simétrica con cifrado por bloques desarrollado por Counterpane Labs y presentado al concurso del NIST que buscaba un sustituto para DES. El tamaño de bloque en Twofish es de 128 bits y el tamaño de clave puede llegar hasta 256 bits.

