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: Cuadro Sinoptico Unidad II

FECHA: 15 de Octubre de 2022.

Algoritmos de Claves Simetricas

- . DES – El estándar de encriptación 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 descifrado). La combinación entre sustituciones y permutaciones se llama cifrado del producto.
- AES – El estándar de encriptación avanzada
  - 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 Su tamaño de clave mayor hace que sea esencialmente irrompible, lo que significa que, incluso si nuestros servidores fueran hackeados, tus datos serían imposibles de descifrar. AES tiene 10 rondas para llaves de 128 bits, 12 rondas para llaves de 192 bits y 14 rondas para llaves de 256 bits
- Modos de cifrado
  - Modo de cifra ECB. electronic codebook mode.
  - Modo de cifra CBC. cipherblock chaining mode.
  - Modo de cifra CFB. cipher feedback mode.
  - Modo de cifra OFB. output feedback mode.
- Otros cifrados
  - Cifrado por transposición o permutación
  - Cifrado Vernam
- Criptoanálisis
  - El criptoanálisis es el arte de descifrar comunicaciones encriptadas sin conocer las llaves correctas. Existen muchas técnicas criptoanalíticas.
    - Ataques a textos cifrados Ciphertext-only attack
    - Ataques de texto plano conocidos
    - Ataques de texto plano seleccionado
    - Ataque del hombre en el medio
    - Ataques contra el hardware o utilizando el hardware base