Supernota

Nombre del alumno: Yahir Aguilar Sicalhua.
Nombre del tema: Unidad II. Algoritmos de Claves Simétricas.
Parcial: 1.
Nombre de la materia: Redes de Computadoras III.
Nombre del profesor: Jorge Alberto Hernández Pérez.
Nombre de la licenciatura: Ingeniería en Sistemas Computacionales.
Cuatrimestre:7.

Algoritmos de Claves Simétricas.

Fuentes de información:

https://platformaeducativauds.com.mx/libro.php?idLibro=169749091116

https://www.ibm.com/mx-es/topics/encryption#:~:text=Est%C3%A1ndares%20de%20cifrado%20de%20datos,utilizando%20claves%20de%2048%20bits

DES – El estándar de encriptación de datos.

Es un algoritmo de cifrado de bloques de cifrado de bajo nivel que convierte texto sin formato en bloques de 64 bits y los convierte en texto cifrado utilizando claves de 48 bits.

Modos de cifrado.

1. Modo de cifra ECB. electronic codebook mode.
2. Modo de cifra CBC. cipherblock chaining mode.
3. Modo de cifra CFB. cipher feedback mode.
4. Modo de cifra OFB. output feedback mode.

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. Para ello, utiliza una clave criptográfica específica, que es efectivamente un conjunto de protocolos para manipular información. Esta clave puede ser de 128, 192 o 256 bits de tamaño.

Chacha20.

El algoritmo ChaCha20 es un algoritmo de cifrado simétrico que soporta claves de 128 y 256 bits y de alta velocidad, a diferencia de AES que es un cifrado por bloques, ChaCha20 es un cifrado de flujo.

Cifrado TwoFish.

Estamos ante un cifrado de clave simétrica, que dispone de un tamaño de bloque de 128 bits, lo que puede verse a priori, como muy seguro ante ataques de fuerza bruta, al requerir grandes capacidades de procesamiento para poder descifrarlo.