NOMNRE DEL ALUMNO: EDDI DAVID AGULAR MARTINEZ

NOMBRE DEL PROFESOR: JORGE ALBERTO HERNANDEZ PEREZ

MARERIA: REDES DE COMPUTADORAS III

TIPO DE TRABAJO: SUPERNOTA

LICENCIATURA: INGENIERIA EN SISTEMAS COMPUTACIONALES

CUATRIMESTRE: 7

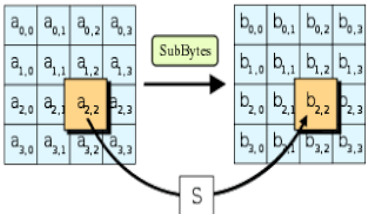
El estándar de encriptación de datos

DES – El estándar de encriptación de datos

El DES fue estandarizado por el ANSI (American National Standard Institute, en castellano: Instituto Nacional Americano de Normalización) bajo el nombre de ANSI X3.92, más conocido como DEA (Data Encrytion Algorithm, en castellano: Algoritmo de Cifrado de Datos)

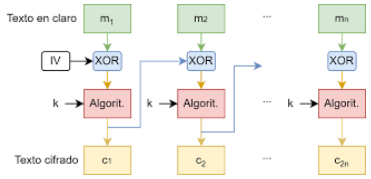
AES – El estándar de encriptación avanzada

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.



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. Suponemos que el algoritmo de cifrado es, que el de descifrado es, que cada bloque de texto plano lo llamamos, y cada bloque de texto cifrado.

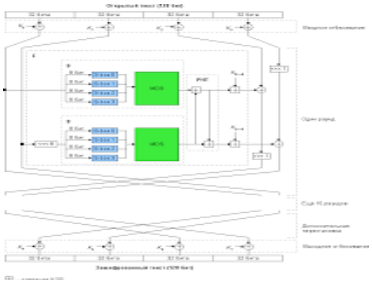


Chacha204

ChaCha20: es un algoritmo de cifrado simétrico, 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

de este cifrado, es de qué se compone. 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. La longitud de su clave puede variar entre los 128, 192 o 256 bits. Es de código abierto, y su uso es totalmente gratuito.



FUENTES DE IINFORMACION.

- https://plataformaeducativauds.com.mx/assets/docs/libro/ISC/876e6c2bdd20ba64820e9d099bd430cf-LC-ISC701%20REDES%20DE%20COMPUTADORAS%20III.pdf