Universidad del Valle De Guatemala

Facultad de Ingeniería

Computación Paralela y Distribuida

Proyecto 2

Programación Paralela con OpenMPI

Elean Rivas 19062
Diego Ruiz 18761

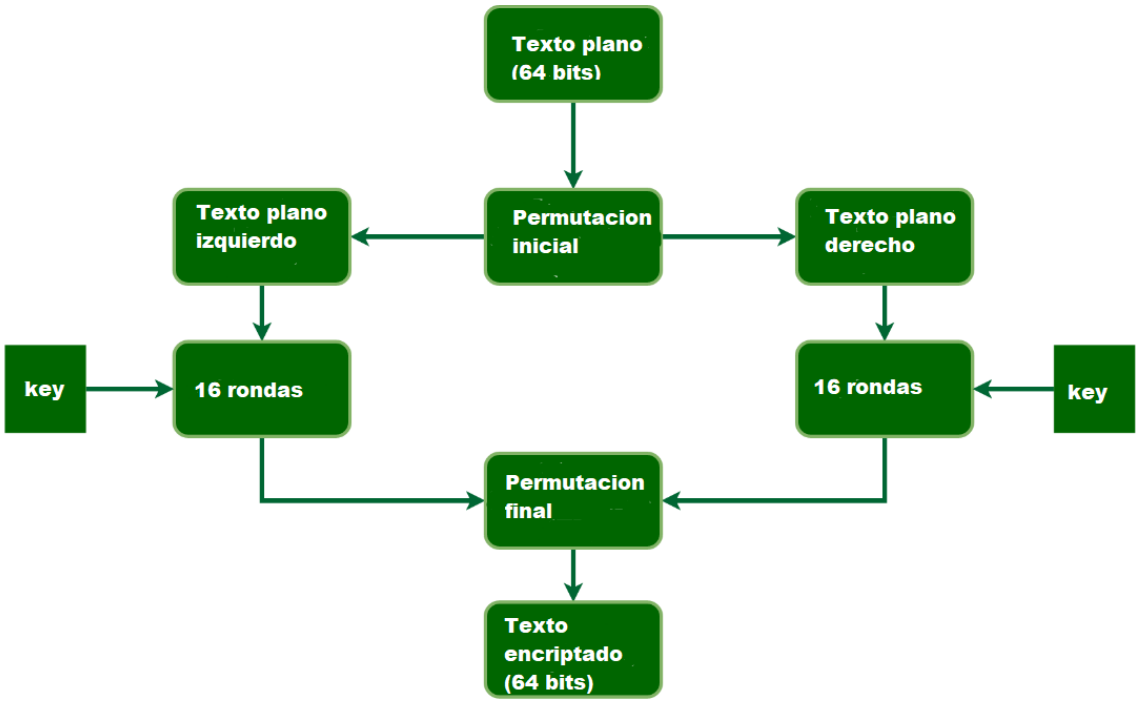
Guatemala, octubre de 2023

DES

Des o Data Encryption Standard, es un una vieja práctica de cifrado de información, en esta se cifra la información en bloques de 56 bits pues el octavo bit de cada combinación es eliminado para generar la clave de 56 bits, es decir la cadena original consta de 64 bits donde el bit 8, 16, 24, 32, 40, 48, 56 y 64 son descartados.

El DES se basa en dos conceptos básicos, sustitución y desplazamiento. El DES consta de 16 pasos, cada uno de los cuales se llama una ronda. Cada ronda realiza los pasos de sustitución y transposición. Ahora, discutamos los pasos a un nivel más general en el DES.

En el primer paso, el bloque de texto plano de 64 bits se entrega a una función de Permutación Inicial (IP).
La permutación inicial se realiza en el texto plano.
A continuación, la permutación inicial (IP) produce dos mitades del bloque permutado; llamadas Texto Plano Izquierdo (LPT) y Texto Plano Derecho (RPT).
Ahora, cada LPT y RPT pasan por 16 rondas del proceso de cifrado.
Al final, LPT y RPT se vuelven a unir y se realiza una Permutación Final (FP) en el bloque combinado.
El resultado de este proceso produce un cifrado de 64 bits.



DES, es característico por ser el primer proceso de encriptación comercial usado, hoy día no se usa pues es muy vulnerable precisamente a algoritmos como bruteforce, que son capaces de generar muchas combinaciones para obtener la información, por tanto bruteforce es el algoritmo perfecto para paralelizar y optimizar si se quiere romper con el paradigma de encriptación DES

referencias:

https://www.techtarget.com/searchsecurity/definition/Data-Encryption-Standard
https://www.tutorialspoint.com/cryptography/data_encryption_standard.html