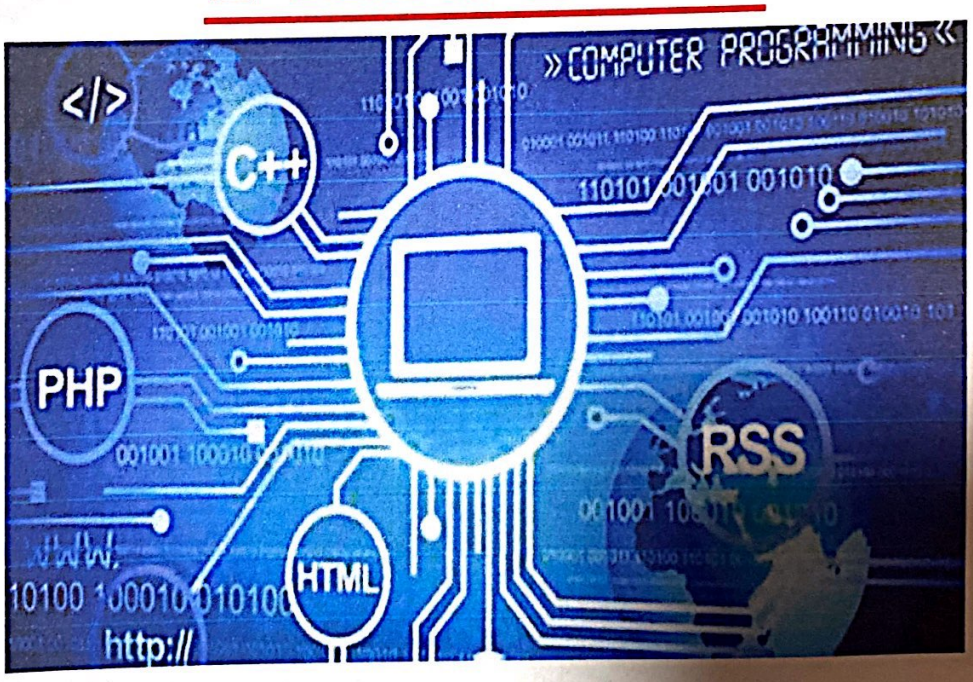
TRABAJO PRACTICO

CIFRADO FEISTEL



ADRIAN FLORES EDDY BEYMAR

6TO DE SECUNDARIA

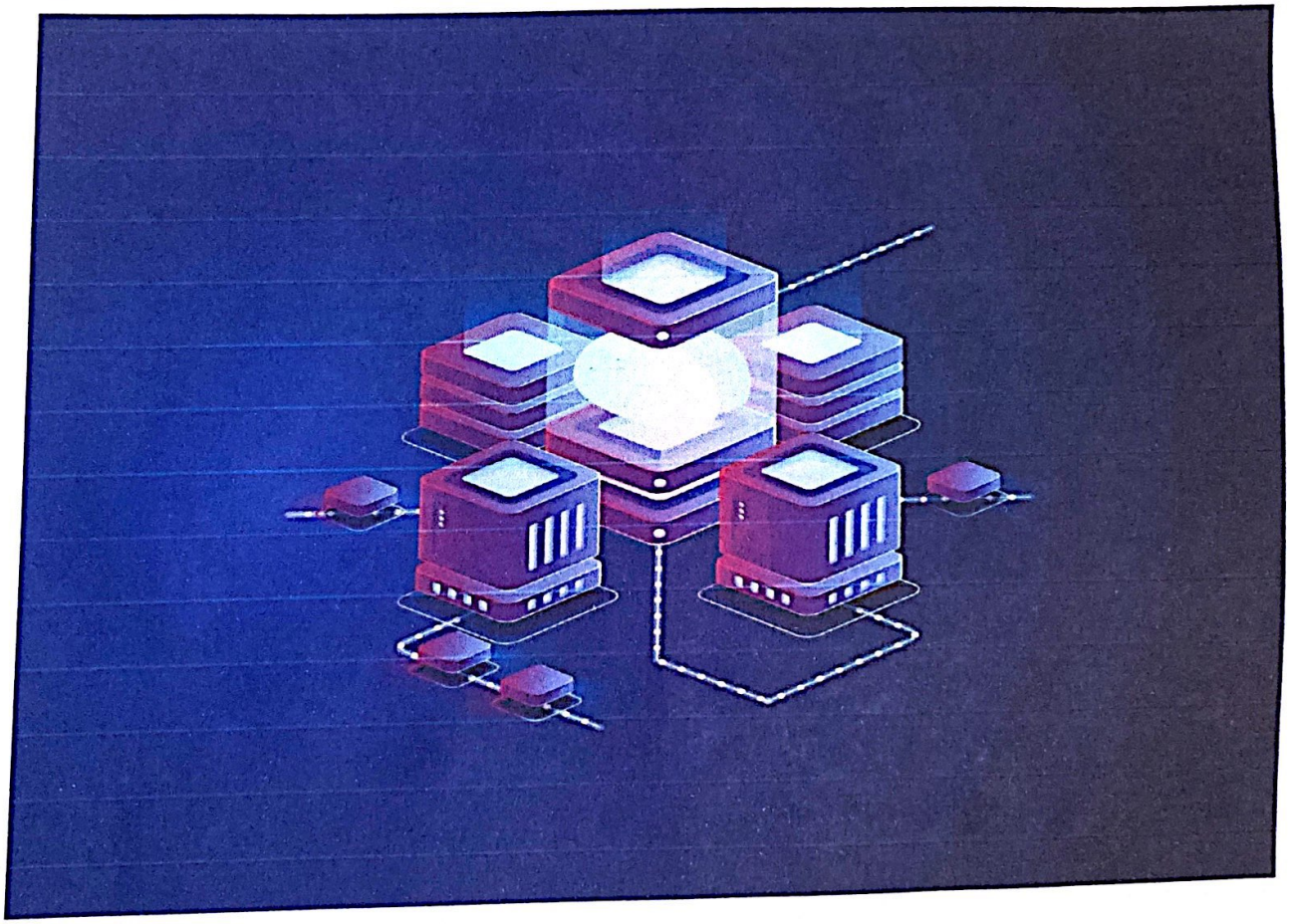
Tema: _____

Fecha: __/__/__

TOP

Cifrado de feistel

El cifrado de Feistel es un metodo de cifrado en bloque y deve su nombre a un criptografo de IBM Horst Feistel y se usa en varios algoritmos de encriptación por bloques donde el mas conocido es el Data Encryption Estandart



El algoritmo

Este algoritmo se denomina simetrico por rondas es decir se realiza siempre las mismas Operaciones un numero determinado de veces denominadas rondas los pasos de la red de Feistel son entre algunos mas

Tema:

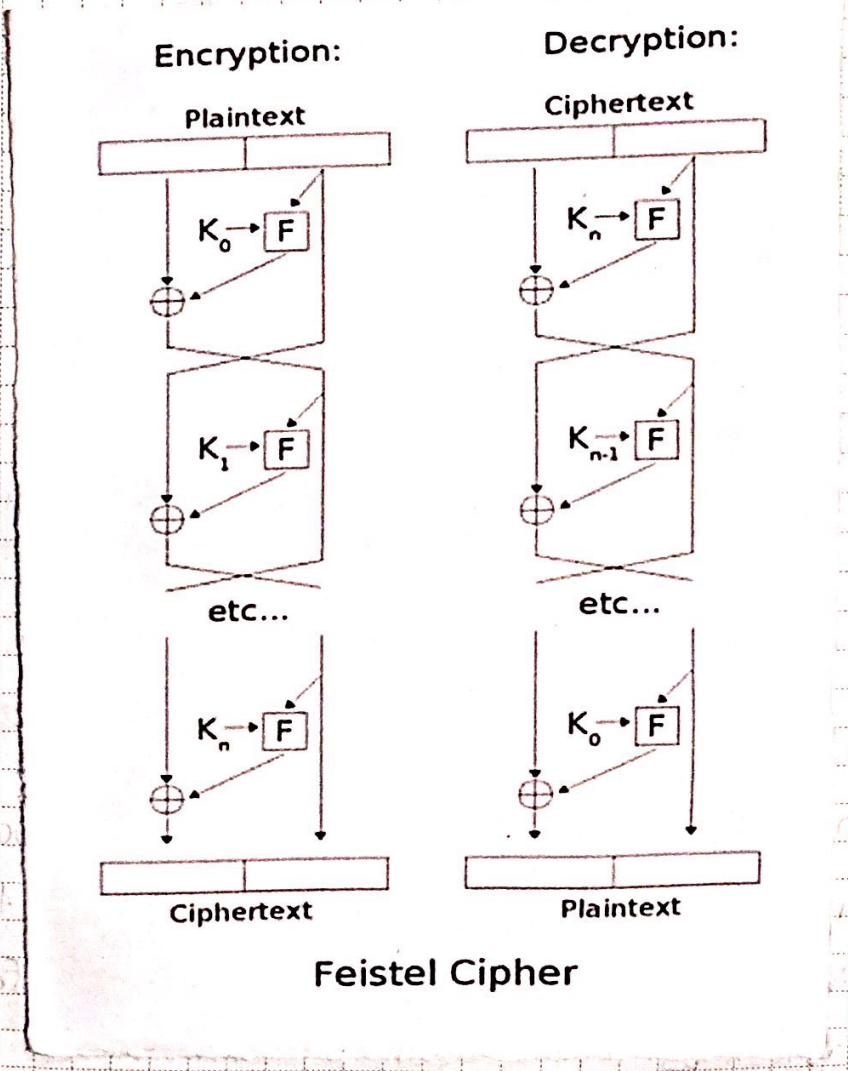
Fecha: / /

Las operaciones basicas de una red de Feistel son las siguientes se descompone el texto plano en dos piezas iguales (L_0, R_0) Para realizar el cifrado en cada ronda $i = 0, 1, 2, \ldots, n-1$ se calcula

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Otra forma de ver el algoritmo es con esta imagen la cual utilize para guiarme al hacer el codigo



Feistel Cipher