Universidad Nacional Autónoma de México

Facultad de Ingeniería

Práctica 3
"Simplified DES"

Criptografía

Grupo: 02

Profesora: Rocío Aldeco, PhD

Elaborado por:
Medel Sánchez Berenice

Semestre 2020-2

Cd. Universitaria a 25 de Febrero del 2020

Objetivo.

Entender el funcionamiento de los algoritmos de cifrado por bloque, así como la utilización de la función Feistel.

Actividades.

- ¿Qué lenguaje de programación es el más adecuado para implementar el algoritmo?
  Debido a que el algoritmo trabaja con bits, el mejor lenguaje por facilidad para implementarlo, sería el lenguaje C. Sin embargo, Python también nos permite realizar las mismas operaciones y la manipulación de cadenas y listas es más fácil.

- Crear el pseudocódigo para descifrar sDES
  INICIO
    LEER
    Key, ciphertext
    CREAR arreglo de subkeys
    Invertir Orden de las llaves

    Llevar a cabo permutación inicial a cipherthext([1,5,2,0,3,7,4,6])
    Separar en dos partes la permutación anterior
    Aplicar la operación feistel con la llave 1
    Separar el resultado de la operación feistel en 2
    Invertir mitad derecha y la mitad izquierda
    Aplicar la operación feistel con la llave 2
    Aplicar la permutación final

  FIN

Conclusiones.

El algoritmo sDES es fácil de implementar debido a las operaciones a nivel de bits que se ocupan, como son la operación xor o las permutaciones de bits. Se entendió que el descifrado se lleva a cabo de la misma forma que el cifrado, simplemente aplicando las llaves en un orden inverso, lo cual hace que la seguridad del algoritmo sea dependiente de la llave inicial. Se aplicó y entendió el funcionamiento de las operaciones feistel, que consiste en la expansión de una mitad de bloque de datos, la combinación con una llave dada, la sustitución con ayuda de los s-boxes, así como una permutación final.