Guzmán Sánchez José Emmanuel
Criptografía

# Simplified DES

1.- Con la descripción dada del algoritmo sDES, ¿Cómo se implementaría y cuál sería el mejor lenguaje de programación para hacerlo?

Python es un lenguaje que es muy flexible con las estructuras de datos, por lo que su manipulación es sencilla, en este caso se hará uso de listas, por lo que se ajusta a las necesidades. Sin embargo, debido a que se hacen operaciones bit a bit, convendría usar un lenguaje de más bajo nivel, como C o VHDL, que nos permite hacer este tipo de operaciones sin mucha complicación.

Una manera sencilla de implementar es por módulos, es decir, distribuir las operaciones entre varias funciones y al final sólo ocupar los resultados. En este caso, conviene usar las siguientes funciones:

- Generador de llaves: Será la función que generé ambas llaves para el algoritmo
- Función *mixing*: Es la que hará la expansión de los bloques y la búsqueda en los S-box
- *Main*: Será la función que haga las permutación y el reacomodo de los resultados de las funciones anteriores

Lo anterior permitirá que el proceso de cifrado y descifrado sea más sencillo, ya que el procedimiento es similar en ambos casos.

2.- ¿Cuál es el proceso a seguir para descifrar un mensaje?

Para descifrar un mensaje mediante DES es importante tomar en cuenta 2 aspectos.

- La función *XOR* es una función involutiva, es decir, es su propia inversa
- El cifrado de una mensaje se basa en la operación y no en el proceso

Tomando en cuenta lo anterior, el descifrado del mensaje se realiza de la siguiente manera.

- Se realiza la misma permutación inicial que en el cifrado, debido a que en éste proceso, al final se aplica una permutación inversa
- Se aplica la función *mixing* para el primer round, sólo que en vez de enviar $K_1$ se envía $K_2$
- Se permutan ambas mitades del resultado anterior
- Se aplica la función *mixing* para el segundo round, y en este caso se envía $K_2$ en vez de $K_1$
- Finalmente se aplica la permutación inversa

La ventaja de usar la operación XOR para un algoritmo de cifrado es que se aplica el mismo proceso, en el mismo orden para el descifrado, sólo cambian los valores de entrada, en este caso las llaves $K_1$ y $K_2$ cambian de orden.