Universidad Nacional Autónoma de México

Facultad de Ingeniería

Práctica 2
"RC4"

Criptografía

Grupo: 02

Profesora: Rocío Aldeco, PhD

Elaborado por:
Medel Sánchez Berenice

Semestre 2020-2

Cd. Universitaria a 18 de Febrero del 2020

Objetivo.

Entender el funcionamiento de los algoritmos de cifrado por flujo, así como implementar el algoritmo RC4 en el lenguaje de programación indicado.

Actividades.

- ¿Qué lenguaje de programación es el más adecuado para implementar el algoritmo?
  El algoritmo se implementará en Python debido a que la conversión de caracteres a código ASCII y viceversa se realizan de manera sencilla con las funciones “ord” y “chr”. Además, la conversión de ASCII a hexadecimal también es sencilla. Y finalmente, el manejo de cadenas es bastante fácil.

- Crear el pseudocódigo para descifrar RC4
  Se lee el mensaje cifrado y se convierte a ASCII, posteriormente se aplican los mismos pasos que para el cifrado y finalmente se imprime el carácter del ascii que genera PRGA.

```
INICIO
        LEER
        Key, ciphertext
        S = []
        //convertir ciphertext de hexadecimal a ascii

        //CREAR arreglo de permutaciones S con la llave de cifrado (igual que en el cifrado)

        FOR i desde 0 hasta 255
                S[i] = i
        FIN
        j  = 0
        FOR i desde 0 hasta 255
                J = (j + S[i] + key[i mod longitudKey]) mod 256
                Intercambiar valores de S[i] y S[j]
        FIN
        //Aplicar PRGA

        i=0, j = 0
        WHILE ciphertext:
                I =(i + 1) mod 256
                J = (j + S[i]) mod 256
                Intercambiar valores de S[i] y S[j]
                V = S[(S[i] + S[j]) mod 256]
                Imprimir caracter cuyo ascii es V
        END
FIN
```

Conclusiones.

El algoritmo RC4 es un algoritmo de encriptado por flujo que utiliza el mismo procedimiento para cifrado y descifrado, por lo tanto, depende de la llave con la que se cifre para ser descifrado y no del procedimiento. Además es bastante fácil de implementar, se ocupan las conversiones de carácter a ascii, de ascii a hexadecimal, la operación xor y permutaciones. Se observó cómo se genera un nuevo mensaje combinando el mensaje en claro con un flujo de caracteres creados a partir de la llave dada.