Guzmán Sánchez José Emmanuel
Criptografía

Algoritmo RC4

1.- Con la descripción dada del algoritmo RC4, ¿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.

- KSA

```
key = input()
S = [i for i in range(256)]
j = 0
for i in range(256):
        j = (j + S[i] + ord(key[ i % len(key) ])) % 256
        S[i], S[j] = S[j], S[i]
```

- PRGA

```
i, j = 0, 0
output = ‘’
while message:
        i = ( i + 1) % 256
        j = ( j + S[i] )% 256
        S[i], S[j] = S[j], S[i]
        k = S[( S[i] + S[j] ) % 256]
        output += hex(k).split('x')[-1]
        message = message[1: ]
```

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

Para descifrar un mensaje mediante RC4 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.

- Generar la *keystream* con el mismo proceso que en el cifrado; usando *KSA* y *PRGA*
- Realizar la operación *XOR* byte a byte de la *key stream* con el mensaje cifrado
- Cada operación realizada dará un carácter del mensaje en claro