

PRÁCTICA: CIFRADO RC4

Objetivo:

Implementar el cifrado en flujo RC4 en el lenguaje de programación que deseen.

Desarrollo:

Implementa el cifrado RC4 según la descripción incluida en las transparencias.
Debe ser válido para cualquier longitud de clave y texto original.

Ejemplo:

Entrada:

Semilla de clave= 2, 5

Texto original= 1, 34

Salida:

Inicialización:

S= [0, 1, 2, 3,..., 255]

K= [2, 5, 2, 5,...,2,5]

S[0]= 0, K[0]= 2 produce f= 2, S[0]= 2, S[2]= 0

S[1]= 1, K[1]= 5 produce f= 8, S[1]= 8, S[8]= 1

S[2]= 0, K[2]= 2 produce f= 10, S[2]= 10, S[10]= 0

...

S[254]= 205, K[254]= 2 produce f= 63, S[254]= 153, S[14]= 205

S[255]= 176, K[255]= 5 produce f= 14, S[255]= 91, S[195]= 176

S= [2, 133, 10, 77, 204, 34, 187, 54, 51, 71, 73, 98, 147,..., 178, 250, 59, 74, 153, 91]

Generación de secuencia cifrante y texto cifrado:

Byte 1 de secuencia cifrante: Salida= S[88]= 144:

10010000

Byte 1 de texto original: Entrada: M[1]=1:

00000001

Byte 1 de texto cifrado: Salida= C[1]= 145:

10010001

Byte 2 de secuencia cifrante: Salida= S[182]= 14:

00001110

Byte 2 de texto original: Entrada: M[2]=34:

00100010

Byte 2 de texto cifrado: Salida= C[2]= 44:

00101100