

PRÁCTICA: CIFRADO DE VERNAM

Objetivo: Implementar el cifrado de Vernam.

Desarrollo:

Implementa en el lenguaje que prefieras el cifrado y descifrado de Vernam según la descripción que se incluye a continuación:

- El cifrado opera bit a bit, mediante la operación XOR entre el mensaje original y la clave aleatoria.
- El descifrado opera bit a bit, mediante la operación XOR entre el mensaje cifrado y la clave aleatoria.

Utiliza código ASCII para pasar de letras a bytes y viceversa, cuando se trate de caracteres imprimibles.

Ejemplos:

Entrada:

Mensaje original: SOL

Salida:

Mensaje original en binario: 010100110100111101001100

Longitud del mensaje binario: 24

Entrada:

Clave aleatoria: 001111000001100001110011

Salida:

Mensaje cifrado en binario: 011011110101011100111111

Mensaje cifrado: oW?

Entrada:

Mensaje cifrado: [t

Salida:

Mensaje cifrado en binario: 0101101101110100

Longitud del mensaje binario: 16

Entrada:

Clave aleatoria: 0000111100100001

Salida:

Mensaje original en binario: 0101010001010101

Mensaje original: TU