

PRÁCTICA: CIFRADO DE VIGENERE

Objetivo: Implementar el cifrado de Vigenere.

Desarrollo:

Implementa el cifrado y descifrado de Vigenere según la descripción que se incluye a continuación:

Se usará el alfabeto sin Ñ, con W y sin espacios, luego el módulo para las operaciones será $m=26$.

El cifrado opera sobre bloques de letras, y la clave es una palabra o frase que se repite cuantas veces sea necesario.

Si la clave tiene longitud r , entonces el texto se divide en bloques de longitud r y la clave se suma a cada bloque, sumando letra a letra módulo 26, para producir el texto cifrado.

Dicho de otra forma, dada la clave $k_1 k_2 \dots k_r$ introducida por el usuario, la primera letra del texto original introducido por el usuario se sustituye por otra que ocupa k_1 posiciones más allá en el alfabeto, la segunda por la que ocupa k_2 posiciones más allá, y así sucesivamente.

Ejemplo:

Palabra clave: MISION

Texto original: ESTE MENSAJE SE AUTODESTRUIRA

| | | | | |
|--------|--------|--------|--------|----|
| ESTEME | NSAJES | EAUTOD | ESTRUI | RA |
| MISION | MISION | MISION | MISION | MI |
| QALMAR | ZASRSF | QIMBCQ | QALZIV | DI |

Texto cifrado: QALMARZASRSFQIMBCQQALZIVDI