

Práctica 06: Cifrado de Sustitución Monoalfabética y de Vigenère

miércoles 10 de abril

APELLIDOS: NOMBRE:

APELLIDOS: NOMBRE:

GRUPO:

AVISO: Los mensajes cifrados los podéis encontrar en el archivo *datos_06_miercoles*.

AVISO: Para escribir los mensajes en claro tenéis que considerar los dos espacios como un cambio de línea.

Para encriptar la información escrita en el alfabeto \mathcal{A}

$\mathcal{A} = \text{"aábcdeéfgghiíjklmnñoópqrstuúvwxyzAÁBCDEÉFGHIÍJKLMNÑOÓPQR}$
 $\text{STUÚVWXYZ0123456789 ,.-()}"$

utilizamos la codificación numérica que a cada símbolo α del alfabeto se le asigna el número $n(\alpha) = p(\alpha) - 1$, donde $p(\alpha)$ es la posición que ocupa α dentro del alfabeto.

1. Sabiendo que la función de cifrado usada ha sido una sustitución monoalfabética con clave $[32, 34]$, descifrar el mensaje cifrado *texto_01*.

mensaje en claro

Las cosas podrían haber sucedido de cualquier otra manera y, sin embargo, sucedieron así. Daniel, el Mochuelo, desde el fondo de sus once años, lamentaba el curso de los acontecimientos, aunque lo acatara como una realidad inevitable y fatal.

2. Sabiendo que se ha usado un cifrado de Vigenère con clave *10 de abril*, descifrar el mensaje cifrado *texto_02*.

mensaje en claro

Después de todo, que su padre aspirarara hacer de él algo más que un quesero era un
hecho que honraba a su padre. Pero por lo que a él
afectaba...

3. Sabiendo que para cifrar los mensajes hemos aplicado primero una sustitución monoalfabética con clave [32, 34] y, a continuación, un cifrado de Vigenère con clave *10 de abril* (es decir, una composición de los cifrados anteriores), descifrar el mensaje cifrado *texto_03*.

mensaje en claro

(EL CAMINO, Miguel Delibes, 1920-2010)