

Práctica 06: Cifrado de Sustitución Monoalfabética y de Vigenère

lunes 8 de abril

APELLIDOS: NOMBRE:

APELLIDOS: NOMBRE:

GRUPO:

AVISO: Los mensajes cifrados los podéis encontrar en el archivo *datos_06_lunes*.

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 $[8, 44]$, descifrar el mensaje cifrado *texto_01*.

mensaje en claro

Las matemáticas son como una corriente de agua.

Existen diversas teorías complicadas, es cierto, pero
la lógica básica es muy sencilla.

2. Sabiendo que se ha usado un cifrado de Vigenère con clave *8 de abril*, descifrar el mensaje cifrado *texto_02*.

mensaje en claro

De igual modo
que el agua fluye desde un lugar elevado hacia
otro más bajo tomando la distancia más corta,
sólo hay una corriente matemática.

3. Sabiendo que para cifrar los mensajes hemos aplicado primero una sustitución monoalfabética con clave $[8, 44]$ y, a continuación, un cifrado de Vigenère con clave *8 de abril* (es decir, una composición de los cifrados anteriores), descifrar el mensaje cifrado *texto_03*.

mensaje en claro

(1Q84, Haruki Murakami, Kioto 1949)