Práctica 06: Cifrado de Sustitución Monoalfabética y de Vigenère

martes 9 de abril

Apellidos: ..... Nombre: .....

Apellidos: ..... Nombre: .....

Grupo: .....

AVISO: Los mensajes cifrados los podéis encontrar en el archivo *datos_06_martes*.
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 $\mathcal{A}$

> $\mathcal{A}$ = "aáb cdeéfghiíjklmnñoópqrstuúvwxyzAÁBCDEÉFGHIÍJKLMNÑOÓPQR 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 $[16, 62]$, descifrar el mensaje cifrado *texto_01*.

mensaje en claro

Borja tenía quince años y yo catorce, y estábamos
allí a la fuerza. Nos aburríamos y nos exasperábamos
a partes iguales, en medio de la calma aceitosa,
de la hipócrita paz de la isla.

2. Sabiendo que se ha usado un cifrado de Vigenère con clave *09 de abril*, descifrar el mensaje cifrado *texto*_02.

mensaje en claro

Nuestras vacaciones
se vieron sorprendidas por una guerra que aparecía fantasmal, lejana y próxima a un tiempo, quizá más temida por invisible.

3. Sabiendo que para cifrar los mensajes hemos aplicado primero una sustitución monoalfabética con clave $[16, 62]$ y, a continuación, un cifrado de Vigenère con clave *09 de abril* (es decir, una composición de los cifrados anteriores), descifrar el mensaje cifrado *texto*_03.

mensaje en claro

(PRIMERA MEMORIA, Ana María Matute, 1925-2014)