

CIFRADOS POR SUSTITUCIÓN POLIALFABÉTICA: VIGENÈRE

En esta práctica vamos a cifrar y descifrar mensajes usando sistemas criptográficos basados en la técnica criptográfica de sustitución polialfabética de Vigenère. La usaremos en dos modalidades: la versión clásica y una versión en flujo. En los ejemplos de la práctica los mensajes están escritos en el alfabeto

$\mathcal{A} = \text{“abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ$
 $\text{áéíóúÁÉÍÓÚ0123456789_.,:;!-¿?()”}$

(alfabeto disponible en el fichero datos.txt en moodle)

DESCRIPCIÓN DE LOS CIFRADOS. Supongamos que tenemos un mensaje en claro M de longitud n escrito en el alfabeto \mathcal{A} (alfabeto con 84 símbolos). Para cifrar M fijamos una clave de cifrado K , que va a ser un mensaje de longitud s escrito en el alfabeto \mathcal{A} . El cifrado de M con clave K sigue los siguientes pasos:

- **Codificación numérica.** A cada símbolo α del alfabeto \mathcal{A} se le asigna el número $n(\alpha) = p(\alpha) - 1$, donde $p(\alpha)$ es la posición que ocupa α dentro del alfabeto ($0 \leq n(\alpha) \leq 83$). Si aplicamos la codificación numérica a M y a K obtenemos dos vectores en \mathbb{Z}_{84} , \underline{m} de longitud n y \underline{k} de longitud s (normalmente $s \leq n$).
- **Cifrado de Vigenère.** El método consiste en sumar, en \mathbb{Z}_{84} , al mensaje numérico \underline{m} una clave extendida \underline{k}^* que se construye a partir de \underline{k} y tiene longitud n (la longitud del mensaje a cifrar)

$$\underline{m} + \underline{k}^* \quad \text{suma en } (\mathbb{Z}_{84})^n$$

La construcción de la clave extendida la vamos a realizar de dos formas:

Versión clásica. En este caso, la clave extendida \underline{k}^* se construye mediante una repetición cíclica de \underline{k} .

Versión en flujo. En este caso, la clave extendida \underline{k}^* se construye con una ecuación de recurrencia lineal y homogénea. En concreto, en este caso usaremos la ecuación de recurrencia

$$x_i = k_1 x_{i-1} + k_2 x_{i-2} + \dots + k_s x_{i-s} \quad \text{con } i \geq s + 1$$

donde

$$(k_1, k_2, \dots, k_s)$$

es la codificación numérica de la clave de partida. Es decir, los siguientes datos para la clave extendida son

$$\begin{aligned} k_{s+1} &= k_1 k_s + k_2 k_{s-1} + \dots + k_s k_1 \\ k_{s+2} &= k_1 k_{s+1} + k_2 k_s + \dots + k_s k_2 \\ &\vdots \end{aligned}$$

- **Decodificación numérica.** Se la aplicamos al mensaje numérico cifrado, $\underline{m} + \underline{k}^*$, para obtener un mensaje cifrado escrito en el alfabeto \mathcal{A} .

Para descifrar los mensajes cifrados usaremos la clave de cifrado extendida con la operación de restar en vez de sumar.

PROBLEMA 1

Sabemos que un mensaje M , escrito en el alfabeto \mathcal{A} , se ha cifrado usando Vigenère con clave K_1 (ver fichero *datos.txt* en moodle) y clave extendida con la versión clásica. Si el mensaje cifrado es el indicado en el fichero de datos, obtener el mensaje original y apuntar sus líneas 1, 4 y 8.

líneas 1, 4 y 8 del mensaje original

Nota: Cuando en el mensaje original aparezcan dos espacios consecutivos lo imprimimos como un cambio de línea.

PROBLEMA 2

Sabemos que un mensaje M , escrito en el alfabeto \mathcal{A} , se ha cifrado usando Vigenère con clave K_2 (ver fichero *datos.txt* en moodle) y clave extendida con la versión en flujo especificada en la descripción. Si el mensaje cifrado es el indicado en el fichero de datos, obtener el mensaje original y apuntar sus líneas 1, 5 y 9.

líneas 1, 5 y 9 del mensaje original

Nota: Cuando en el mensaje original aparezcan dos espacios consecutivos lo imprimimos como un cambio de línea.