

## Práctica 06: Sustitución Monoalfabética

semana del 10 de abril

APELLIDOS: ..... NOMBRE: .....

APELLIDOS: ..... NOMBRE: .....

GRUPO: .....

En esta práctica vamos a cifrar y descifrar mensajes usando sistemas criptográficos de clave privada basados en la técnica criptográfica de sustitución monoalfabética. A continuación se describe cómo se puede trabajar algebraicamente con este sistema criptográfico, usando aritmética modular.

Para encriptar la información escrita en el alfabeto  $\mathcal{A}$  formado por los 83 símbolos:

“aábcdeéfgghiíjklmnñoópqrstuúvwxyzAÁBCDEÉFG  
HIÍJKLMNÑOÓPQRSTUÚVWXYZ0123456789 ,.:;-()”

(alfabeto disponible en la variable *alf* del fichero *entrada\_datos\_06.txt*, dentro de la carpeta *práctica 06 de la moodle*)

ciframos cada símbolo del mensaje utilizando el siguiente proceso:

- Codificación numérica: A cada símbolo  $\alpha$  del alfabeto se le asigna el número  $n(\alpha) = p(\alpha) - 1$ , donde  $p(\alpha)$  es la posición que ocupa  $\alpha$  dentro del alfabeto ( $0 \leq n(\alpha) \leq 82$ ).
- Cifrado por sustitución monoalfabética con **clave de cifrado**  $(a, b) \in (\mathbb{Z}_{83})^2$ , descrito en la siguiente función

$$\begin{aligned} f : \mathbb{Z}_{83} &\rightarrow \mathbb{Z}_{83} \\ n &\mapsto an + b \end{aligned}$$

Nota:  $a$  debe ser un elemento de  $\mathbb{Z}_{83}$  con inverso, es decir,  $\text{mcd}(a, 83) = 1$ .

- Decodificación numérica: Proceso inverso al descrito para la codificación numérica.

(el mensaje cifrado es la concatenación del cifrado de los símbolos del mensaje en claro)

Una vez fijada la clave de cifrado, la función sustitución monoalfabética establece una biyección del alfabeto  $\mathcal{A}$  de forma que a cada letra en claro se le asocia de forma única otra letra del alfabeto  $\mathcal{A}$ , letra cifrada. De esta forma, para realizar la operación de descifrado, podríamos optar por almacenar, de forma exhaustiva, dicha biyección. Sin embargo, también podemos optar por describir el proceso de descifrado vía la operación aritmética que permite construir la función inversa  $f^{-1}$ . Es fácil demostrar que  $f^{-1}$  es una sustitución monoalfabética con clave

$$(a^{-1}, -a^{-1}b)$$

denominada **clave de descifrado**.

Si trabajamos con las claves de cifrado y de descifrado, la implementación de los procesos de cifrado y de descifrado no requiere el almacenamiento de la biyección que determina el cambio de alfabeto.

## PROBLEMA 1

Supongamos que un mensaje en claro escrito en el alfabeto *alf* lo ciframos con sustitución monoalfabética y clave  $(20, 23) \in (\mathbb{Z}_{83})^2$ . Si el mensaje cifrado es el dado en la variable *texto\_cifrado\_1* dentro del fichero *entrada\_datos\_06.txt*, obtener el mensaje en claro.

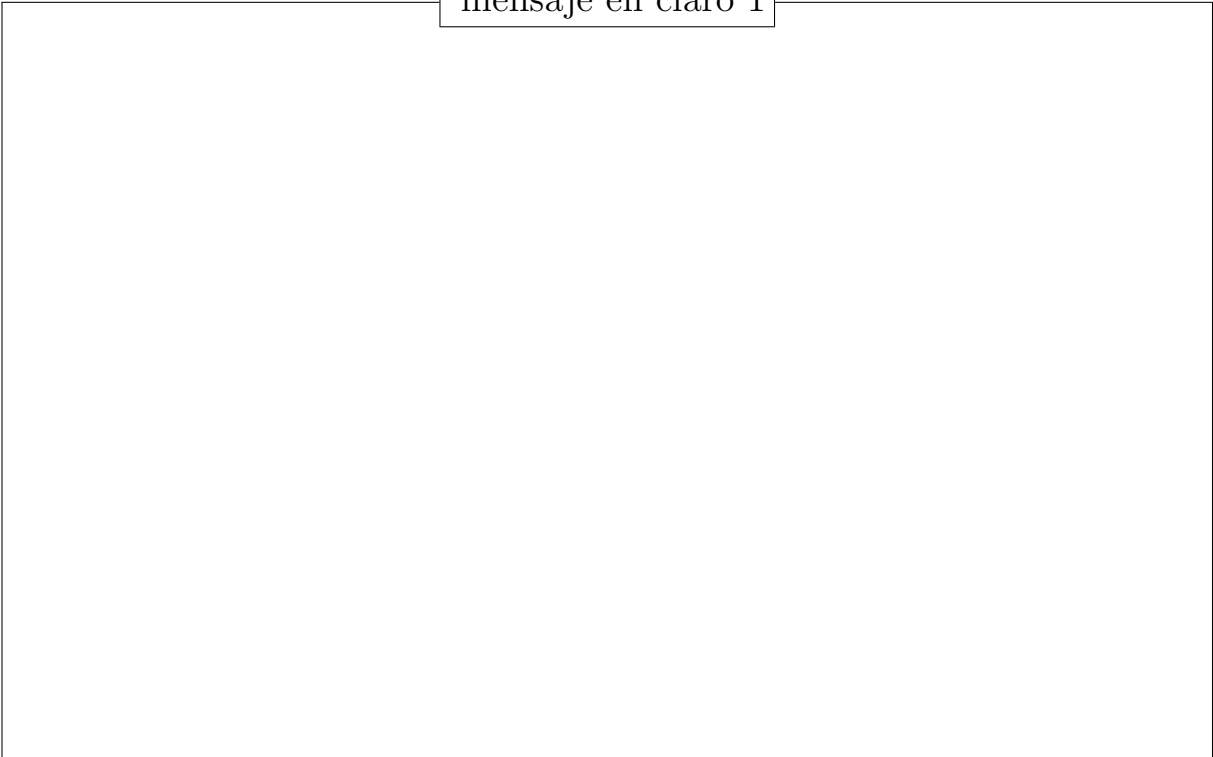
## PROBLEMA 2

Supongamos que un mensaje en claro escrito en el alfabeto *alf* lo ciframos con sustitución monoalfabética de forma que para cada línea del mensaje en claro usamos la **clave de cifrado**

$$(20^i, 23 \cdot i) \in (\mathbb{Z}_{83})^2$$

siendo  $i$  el lugar que ocupa la línea dentro del mensaje en claro (clave inicial  $(20, 23)$  y cada cambio de línea se considera que pertenece a la línea de partida). Si el mensaje cifrado es el dado en la variable *texto\_cifrado\_2* dentro del fichero *entrada\_datos\_06.txt*, obtener el mensaje en claro.

mensaje en claro 1



mensaje en claro 2

