

# PRÁCTICA 1: Criptografía (Parte 1)

Seguridad en Servicios y Aplicaciones  
Curso 2019-2020

Lenguajes y Ciencias de la Computación.  
E.T.S.I. Informática, Universidad de Málaga

### RELACIÓN DE EJERCICIOS:

1. Dado el siguiente código Python, que implementa el cifrado Cesar (+3) para el alfabeto inglés en Mayúsculas ( $C: M \rightarrow M + 3 \pmod{26}$ ),

```
def cifradoCesarAlfabetoInglesMAY(cadena):
    """Devuelve un cifrado Cesar tradicional (+3)"""
    # Definir la nueva cadena resultado
    resultado = ''
    # Realizar el "cifrado", sabiendo que A = 65, Z = 90, a = 97, z = 122
    i = 0
    while i < len(cadena):
        # Recoge el caracter a cifrar
        ordenClaro = ord(cadena[i])
        ordenCifrado = 0
        # Cambia el caracter a cifrar
        if (ordenClaro >= 65 and ordenClaro <= 90):
            ordenCifrado = (((ordenClaro - 65) + 3) % 26) + 65
        # Añade el caracter cifrado al resultado
        resultado = resultado + chr(ordenCifrado)
        i = i + 1
    # devuelve el resultado
    return resultado
```

se pide implementar la siguiente funcionalidad:

- a) Implementar la función de descifrado Cesar para alfabeto inglés en mayúsculas, la cual descifre los textos cifrados creados por el código anterior.
  - b) Modificar las funciones de cifrado y descifrado, para que soporten tanto letras en mayúsculas (A..Z) como letras en minúsculas (a..z) en el alfabeto Inglés.
  - c) Modificar las funciones de cifrado y descifrado, para que soporten el cifrado Cesar generalizado ( $C: M \rightarrow M + i \pmod{26}$ )
2. Implementar en Python las funciones de cifrado y descifrado del cifrado mono-alfabético (ver Tema 2, ejercicio número 3). El cifrado mono-alfabético tiene como entrada el texto en claro y una clave secreta, y se realiza sumando en módulo 26 cada carácter "i" del texto en claro por su correspondiente carácter "i % len(clave)" de la clave secreta.

Por ejemplo, para el texto en claro HOLAAMIGOS y la clave CIFRA, el proceso de cifrado y descifrado es el siguiente:

H	O	L	A	A	M	I	G	O	S
8	15	12	1	1	13	9	7	15	19
C	I	F	R	A	C	I	F	R	A
+3	+9	+6	+18	+1	+3	+9	+6	+18	+1
K	X	R	S	B	P	R	M	G	T
11	24	17	19	2	16	18	13	33→7	20