PRÁCTICA 1: Criptografía (Parte 1)

Seguridad de la Información
Curso 2018-2019

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

PRÁCTICA 1: Criptografía (Parte 1)

Curso: 2018-2019

RELACIÓN DE EJERCICIOS:

1. Dado el siguiente código Python, que implementa el cifrado Cesar (+3) para el alfabeto Inglés en Mayúsculas (C: M → M + 3 (mod. 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) (**4 puntos**) Implementar la función de descifrado Cesar para alfabeto Inglés en mayúsculas, la cual descifre los textos cifrados creados por el código anterior.

b) (**2 puntos**) 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) (**2 puntos**) Modificar las funciones de cifrado y descifrado, para que soporten el cifrado Cesar generalizado (C: M → M + i (mod. 26))

2. (**2 puntos**) Implementar en Python las funciones de cifrado y descifrado del cifrado monoalfabético (ver Tema 2, ejercicio número 3). El cifrado monoalfabético 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
7	14	11	0	0	12	8	6	14	18
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**
10	23	17	18	1	15	17	12	32→6	19