Ejercicios

Ejercicio1. Código César

En criptografía, el **cifrado César** es uno de los más usados principalmente por que es una manera sencilla de codificar texto. También se le conoce como **cifrado por sustitución** y consiste en que una letra en el texto original es reemplazada por otra letra que se encuentra a un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A).

Texto original: `ABCDEFGHIJKLMNÑOPQRSTUVWXYZ`

Texto cifrado: `DEFGHIJKLMNÑOPQRSTUVWXYZABC`

Este método de cifrado lleva el nombre de Julio César que según la tradición fue el primero en utilizarlo para comunicarse con sus generales. Julio César usaba un desplazamiento de 3 posiciones para codificar los mensajes.

No se sabe si era efectivo este cifrado para la época, pero debió ser bastante seguro: primero, porque la mayoría de sus enemigos no sabían ni leer y, segundo, porque el atacante debería hacer un análisis criptográfico del texto para leer el mensaje correctamente.

Realiza un programa al que se le pasen **dos argumentos**: el nombre de *un archivo de texto* y un *número* entre el 1 y el 9. Por ejemplo:

```
> cifrado prueba.txt 4
```

El programa usará el número para cifrar el texto del archivo tantas posiciones como dice el número.

El resultado se guardará en un archivo con el nombre igual que el original pero con la extensión **`cfN`**, donde la **`N`** representa el número de posiciones de la codificación. En el ejemplo, se llamará `prueba.cf4`

Nuestro programa debe gestionar todas las excepciones que se os ocurran: que no hay dos argumentos; el fichero original exista; que el argumento de posiciones sea un número y entre 1 y 9; avisar si el archivo ya fue codificado con ese cifrado,…

Nota. Aunque la RAE se sienta perjudicada en su defensa de la lengua castellana y, otras latinas, desgraciadamente el idioma anglosajón domina las tecnologías del mundo por lo que supondremos que nuestros textos no contendrán caracteres no incluídos en el inglés

Ejercicio2. Código César (parte2)

Realiza otro programa que permita descifrar los códigos César. En este caso sólo se le pasa un argumento con el nombre del archivo encriptado y por la extensión se deducirá que desplazamiento se le ha aplicado y guardará el archivo descifrado.

```
> descifrado prueba.cf2
```