

CIFRADOS CLÁSICOS

El objetivo de esta práctica es criptoanalizar una serie de ficheros que se han obtenido a partir de un texto en español que se ha cifrado mediante algún cifrado clásico (sustitución monoalfabética, polialfabética o transposición).

A estos ficheros, previamente se le han suprimido los espacios, signos de puntuación, saltos de línea, cifras, etc. Únicamente se han quedado los 27 caracteres del alfabeto español y todos en mayúscula.

Para realizar la práctica, hay que pedir que se envíen los textos cifrados.

Una vez recibidos, hay que realizar un análisis del texto para detectar qué sistema de cifrado se ha usado y cuál es la clave.

En el fichero *Funciones.py* se incluyen una serie de funciones (en Python) que pueden ayudar a realizar el criptoanálisis.

Si a la hora de descifrar algún fichero se encuentra alguna dificultad, se puede pedir alguna información adicional sobre qué tipo de documento se ha cifrado y así facilitar el criptoanálisis.

De la práctica hay que entregar:

Los ficheros con los textos descifrados.

Una memoria donde se explique brevemente cómo se ha realizado el criptoanálisis.