

Problema 6. Programa per encriptar i desencriptar

Objectiu

Treballar amb cadenes. Petites idees d'encriptació. Fer recorreguts. Treball amb diccionaris.

Codi d'arrencada

El cònsul i dictador romà Juli Cèsar, va idear un sistema per enviar els seus missatges xifrats, de manera que si algú l'interceptava, no podia entendre el que hi havia escrit.

https://ca.wikipedia.org/wiki/Xifratge_de_C%C3%A8sar

El seu sistema era molt senzill, simplement canviava una lletra per una altra desplaçant-la posicions a l'alfabet.

Aquest codi inicial, permet xifrar un missatge segons el codi de Cèsar:

```
missatge_orig = input ("Entra un text: ")
missatge_xifr = "" # cadena buida pel resultat
clau = 2 # clau per encriptar

for c in missatge_orig: # per tots els caràcters del missatge
    x = ord ( c ) # el passem a numèric
    x = x + clau # sumem la clau
    missatge_xifr = missatge_xifr + (chr(x))
    # anem enganxant al resultat

print (" El missatge encriptat és: ", missatge_xifr )
```

Exercicis proposats

- 1) Executa el programa i comprova que funciona bé. Mireu-vos què fan les funcions de Python `ord ()` i `chr ()`. Podeu provar a canviar la clau.
- 2) Mireu-vos com funciona la codificació dels caràcters. Veieu que al sumar una clau, podem anar a parar a símbols que no són les lletres habituals. Proposeu una forma d'arreglar això.
- 3) Mireu al manual com funcionen uns diccionaris. La codificació de Cèsar és molt fàcil de descodificar, utilitzeu un diccionari per crear un sistema de codificació més hàbil.

Nota: un caràcter pot codificar a més d'un, ex. { 'a': 'fs2' }

- 4) Serieu capaços de fer un programa que donat el missatge encriptat el desencripti?
- 5) Podeu fer un programa d'encriptar i desencriptar fitxers de text?