



La criptografía es el proceso de oscurecer la información para hacerla ilegible si no se tiene cierta información especial. Durante siglos se han estado desarrollando esquemas para encriptar (cifrar) mensajes – unos mejores que otros – pero la llegada de los ordenadores e internet ha revolucionado este campo. Actualmente es difícil no encontrar algún tipo de encriptación en muchos aspectos de nuestras vidas. La encriptación nos permite compartir información con otras personas o entidades de confianza sin temor a que sea revelada.

En este proyecto trabajaremos con el cifrado César. La idea del cifrado César es tomar un entero y desplazar (*shift*) cada letra del mensaje por ese entero. En otras palabras, supóngase que el desplazamiento es  $k$ . Todas las instancias de la  $i$ -ésima letra del alfabeto que aparezca en el texto plano debe convertirse en la  $(i + k)$  letra del alfabeto en el texto cifrado.

Implementaremos funciones tanto para cifrar textos, como para descifrarlos. Con ellas seremos capaces, por ejemplo, de descifrar el siguiente texto encriptado:

```
Cl sl jseyp bc jy Kyla fy, bc  
aswm lmkzpc lm osgcpm yampbypkc,  
lm fy ksafm rgcknm osc tgtiy sl  
fgbyjem bc jmq bc jylxy cl  
yqrgjjcpm, ybypey ylrgey, pmaíl  
djyam w eyjem amppcbmp. Sly mjyy  
bc yjem káq tyay osc aypicpm,  
qyjngaól jyq káq lmafcq, bscjmq  
w osczpylrmq jmq qázybmq,  
jylrchyq jmq tgcplcq, yjeúl  
nyjmkglm bc yáybgbspy jmq  
bmkglemq, amlqskiyl jyq rpcq  
nyprcq bc qs fyagclby.
```



```
En un lugar de la Mancha, de  
cuyo nombre no quiero acordarme,  
no ha mucho tiempo que vivía un  
hidalgo de los de lanza en  
astillero, adarga antigua, rocín  
flaco y galgo corredor. Una olla  
de algo más vaca que carnero,  
salpicón las más noches, duelos  
y quebrantos los sábados,  
lantejas los viernes, algún  
palomino de añadidura los  
domingos, consumían las tres  
partes de su hacienda.
```