

Ejercicio 16: Codificación de mensaje

En este ejercicio vamos a realizar la codificación de un mensaje de texto usando un método que tenían los Romanos. Este método se conoce con el nombre de método de César y consiste en:

En criptografía, el **cifrado César**, también conocido como **cifrado por desplazamiento**, **código de César** o **desplazamiento de César**, es una de las técnicas de cifrado más simples y más usadas. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra 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), la B sería reemplazada por la E, etc. Este método debe su nombre a Julio César, que lo usaba para comunicarse con sus generales.

El cifrado César muchas veces puede formar parte de sistemas más complejos de codificación, como el cifrado Vigenère, e incluso tiene aplicación en el sistema ROT13. Como todos los cifrados de sustitución alfabética simple, el cifrado César se descifra con facilidad y en la práctica no ofrece mucha seguridad en la comunicación.

Realiza un programa que dado un mensaje lo cifre usando el método anterior. Para este métodos puedes usar un string o un vector de string que si no recuerdas se lo puedes decir a tu profesor para que te lo recuerde.

Guarda el ejercicio con el nombre *Pascal16.pas*.