**Cifrado César**

Utilizado por Julio César para comunicarse con sus oficiales, consiste en sustituir cada letra del mensaje por la que está ***n*** posiciones más adelante o atrás en el alfabeto. Si ***n = 3***, la ***A*** se sustituiría por la ***D***, la ***B*** por ***E***, la ***C*** por la ***F*** y así sucesivamente. De este modo, la palabra ***epsilones*** se transforma en ***HSVLORQHV***.

En los sistemas de encriptación se suele distinguir entre el algoritmo o procedimiento general y la clave, que sirve para singularizar el resultado del algoritmo. En el caso del cifrado César, el algoritmo sería la regla por la cuál cambiamos cada carácter por uno que está ***n*** posiciones más adelante, mientras que la clave sería el valor concreto utilizado para ***n***.

Lo malo de este sistema es que, si se sabe que se está utilizando, solo permite 26 sustituciones distintas (tantas como letras tiene el alfabeto), con lo que su descifrado es trivial. Para complicar un poco la cosa se puede utilizar, en vez de una cifra, dos, o más. Así, si la clave es 31, se sustituirá la primera letra por la que esté tres posiciones por delante, la segunda por la que esté una posición más avanzada, la tercera por la que esté tres posiciones por delante, y así sucesivamente.

**Las matemáticas del cifrado César**

Si ***x*** es la posición de la letra que queremos cifrar, la posición de la nueva letra vendrá dada por la fórmula:

$$f(x) = (x + n) \bmod p$$, donde:

***p*** = longitud del alfabeto (generalmente 26),
***x*** = número asociado a la letra (1 para la ***A***, 2 para la ***B***, etc),
***n*** = clave, dependiendo de la cual cambiará el código una vez codificado.

Por ejemplo, si codificamos la palabra clave tomando ***A*** como la posición 1 y haciendo ***n = 5***, se tiene:

$$C \rightarrow f(3) = (3+5) \bmod 26 = 8 \rightarrow H$$
$$L \rightarrow f(12) = (12+5) \bmod 26 = 17 \rightarrow Q$$
$$A \rightarrow f(1) = (1+5) \bmod 26 = 6 \rightarrow F$$
$$V \rightarrow f(22) = (22+5) \bmod 26 = 1 \rightarrow A$$
$$E \rightarrow f(5) = (5+5) \bmod 26 = 10 \rightarrow J$$

Para descifrar algo tan sencillo, utilizamos la fórmula inversa de aquella que hemos utilizado para cifrar (estas funciones siempre han de ser inyectivas):

$$f(x) = (x - n) \bmod p$$

**Ejercicio:** Desarrolle dos programas en lenguaje Java, el primero que implemente el algoritmo descrito mas arriba para codificar un mensaje (debe solicitar el numero ***n)*** y un segundo programa que decodifique un mensaje dado. Para este segundo programa suponga que no conoce el valor ***n*** (clave) del método explicado.

Utilizando el segundo programa decodifique el mensaje siguiente:

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **O** | **O** | **H** | **J** | **X** | **H** | | **Y** | **L** | | **Y** | **H** | **Q** | **F** | **L** |

El espacio en blanco no se codifica.

**Sugerencia:** Utilice arreglos unidimensionales tanto para el mensaje original y como para el nuevo mensaje. Además como se desconoce el valor de la clave (que corresponde al desplazamiento en el alfabeto original) su programa debe generar todas las combinaciones posibles y mostrarlas para que el usuario determine cual es el mensaje correcto.