Claves secretas y encriptamiento de códigos

La aritmética es la ciencia que estudia los números y su desarrollo da lugar a la teoría de números. ¿Qué interés tiene para la vida diaria?
Desde la Antigüedad, se han enviado mensajes que se encontraban escritos en un código oculto y cuya finalidad era que lo entendiera solo el receptor del mensaje. Esta ciencia, llamada criptografía, fue empleada por Julio César o Felipe II, entre otros, para enviar mensajes a sus tropas. El ejército alemán, en la última gran guerra, con la máquina Enigma, generaba mensajes cifrados. El caso de la máquina Enigma ha sido uno de los retos más difíciles resueltos por la criptografía. Su resolución por parte de los británicos fue una de las causas de la derrota alemana en la II Guerra Mundial. Este asunto llevó a Gran Bretaña a construir el Colossus, el primer ordenador del mundo, dedicado exclusivamente a descodificar los mensajes alemanes. Destacó con luz propia en este proyecto el matemático Alan Turing.
Cuando Julio César envía mensajes secretos a sus legiones en la guerra de las Galias, lo hace cambiando el orden de las letras del alfabeto (cifrado César). Este tipo de mensajes es más un problema filológico que matemático. El tipo de clave utilizada en este mensaje es una clave privada. Esto exige acordar previamente la clave con el receptor del mensaje; lo que no es fácil es cómo hacerlo de forma segura. En caso de querer enviar el mensaje a varias personas, la dificultad se incrementa. Por otra parte, si la clave utilizada es descubierta por el interceptor del mensaje, son descifrados inmediatamente todos los mensajes ocultos.

Actualmente, los profesionales de la criptografía se dan cuenta de que al hacer públicas las claves llegan a todos los receptores que sea necesario. Es evidente que el receptor dispone de una clave secreta que le permite descifrar el mensaje público. De esta forma se ha garantizado la emisión de los mensajes a todos los destinatarios sin perjuicio de la seguridad. Esto se conoce como cifrado asimétrico: la clave pública es conocida por todos los usuarios; la clave secreta solo la conoce el receptor.
Este procedimiento es de máxima actualidad, con una implicación directa en nuestra vida diaria, al garantizar la seguridad en Internet y facilitar el comercio electrónico.

Paso 1: **Descifrar y crear un mensaje criptográfico**

El primer paso del proyecto implica descifrar y enviar un mensaje criptográfico, de tipo filológico,
según un código. Nuestra clave secreta consiste en que sustituiremos cada letra del alfabeto por la
que ocupe 5 lugares delante de ella. Completamos el ciclo volviendo a empezar de forma correlativa
a partir de la U, que se transforma en la A.
Escribimos el alfabeto y debajo la letra correspondiente al nuevo código.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E

1. Intenta descifrar el mensaje:
QFY RFZJRFZNHFY YTS RAD NSZJXJYFSZJY
2. Escribe con la clave dada el mensaje:
NO ENTRE AQUÍ QUIEN NO SEPA GEOMETRÍA

3.- Resolve o seguinte criptograma:

```
    A  B C
    A  B C
+   A  B C
_____________
    B  B  B
```

4.- Inventa ti unha linguaxe encriptada e escribe un texto coa mesma, que os demais deberán traducir.

Biografía

Redacta unha pequena biografía sobre Alan Turing.