Si lo escondo, ¿lo encuentras?
Aritmética del reloj

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

Rompiendo la cifra de César

En la primera actividad has aprendido a cifrar por el método de César pero ahora debes jugar un papel diferente, el de espía o criptoanalista, es decir has interceptado un mensaje que va dirigido a otra persona y quieres descifrarlo. Como no va dirigido a ti desconoces la clave (valor del desplazamiento). ¿Qué puedes hacer para descifrarlo?

Un método por fuerza bruta sería probar con todas las posibles claves. Como sólo existe un determinado número de valores de desplazamiento, 27 en español si no se ha desordenado el alfabeto, se pueden probar todos y cada uno de los posibles desplazamientos hasta encontrar un mensaje coherente. Una forma de hacer esto es usar una tabla y en cada renglón se escribe el texto con un desplazamiento diferente. Rellena la tabla

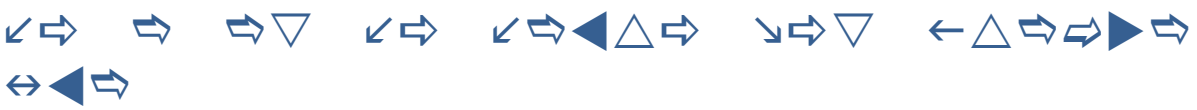
Mensaje cifrado	J	Z	W	J	O	F
d = 1	I	Y	V	I	Ñ	E
d= 2	H	X	U	H	N	D
d= 3						
d = 4						
d = 5						
d = 6						
d = 7						
.....						

¿Has escrito alguna línea con sentido? ¿Cuál es el valor de d en esa línea?, ese valor de d es la clave.

Si encontraste algún material en el maletín del espía que te ayudó para cifrar, piensa que también lo puedes usar para descifrar y rellenar este tipo de tablas de forma más fácil.

Pero está claro que este método no es útil si se sospecha que se está usando un alfabeto desordenado.

Vamos a comprobar que de nuevo las matemáticas son muy útiles para descifrar un mensaje sin necesidad de usar el ataque por fuerza bruta. Para ello te proponemos que descifres el siguiente mensaje:



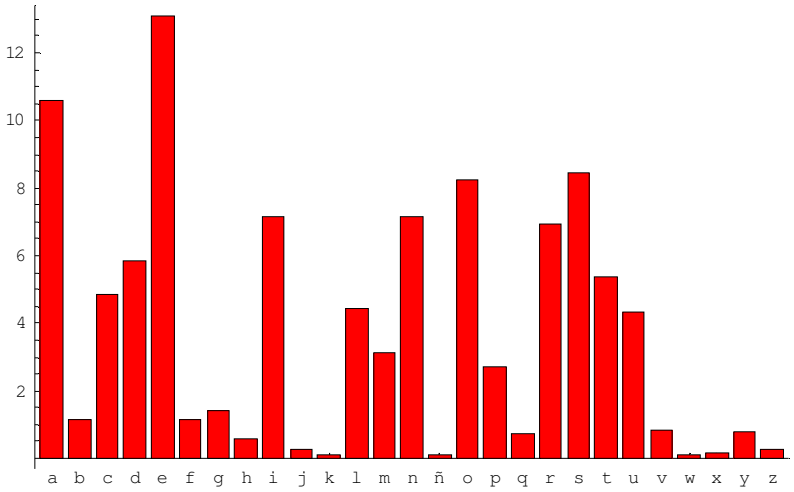
Si este mensaje procede de un mensaje original en el que cada símbolo se ha sustituido siempre por la misma letra el método presenta una debilidad: la frecuencia de aparición de cada letra en el texto claro se refleja exactamente en el criptograma. Es decir, la misma frecuencia que tiene por ejemplo la letra *a* en un texto claro tendría su letra asociada en el texto cifrado. Esto da muchas pistas para

Elaborado por:
Profundiza
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

alguien que lo quiera descifrar: sólo hay que basarse en el estudio de frecuencias y pensar un poco en castellano (bueno cada uno en su idioma).

Aunque no se sabe quién fue el primero en darse cuenta de esta debilidad, la descripción más antigua conocida es del siglo IX y se debe a Al Hindi *el filósofo de los árabes*. Veamos la técnica que usó, conocida como análisis de frecuencias:

1. Hay que establecer la frecuencia de cada letra del alfabeto. La figura muestra los valores, en tanto por ciento, estudiados en archivos de 50.000 caracteres en castellano.



2. Después se examina el texto cifrado y se determina la frecuencia de cada letra. Completa la tabla siguiente

Carácter	↙	⇨	⇨	▽	↙	◀	△	↘	←	⇨	▶	↔
Frecuencia												

3. Es lógico suponer que la letra que más se repite en el texto cifrado procede de la más repetida en nuestro alfabeto.

   También hay que tener en cuenta el sentido común para poder dar sentido al mensaje.

   ¿Has descifrado ya el mensaje? Pues te proponemos otro:

⑩⑥③⑥ ⑥⑤ ⑩❶ ❻❶④⑥

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
Profundiza
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

Seguro que ahora te ha costado más. Hay una razón: es muy probable que los textos largos sigan las frecuencias habituales pero los cortos se desvían de las frecuencias normales. Pero hay que tener cuidado pues esto no es siempre así. Por ejemplo, el autor francés George Perec se dedicó a experimentar con el lenguaje y tiene algunos palíndromos (frases que se leen igual de izquierda a derecha que de derecha a izquierda) increíbles:

O rey, o joyero

Amad a la dama

Somos o no somos.

Este autor escribió *El secuestro* en 1969, y en todo el libro no aparece ni una sola vez la letra "e" (tiene más de 200 páginas). El novelista inglés Gilbert Adair consiguió traducir la obra a su idioma y también consigue que no aparezca la letra *e*. Los traductores al castellano, logran que en el libro no exista la *a*. ¡Menuda forma de estropear el análisis de frecuencias!

En los dos ejemplos anteriores has comprobado que los cifrados por desplazamiento son muy fáciles de romper (basta usar un análisis de frecuencias o un ataque por fuerza bruta). Por esta razón se han sofisticado las técnicas de cifrado. Si te ha gustado el tema puedes investigar un poco en el apartado Para saber más

Elaborado por:
Profundiza
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL