Criptografía para principiantes: Método de la escítala

por
Óscar Carrión Lostal
(IES Valdespartera)

Ya en el primer artículo de la serie criptografía para principiantes, vimos distintos métodos de cifrar y descifrar mensajes, como el de Julio César y el de Vigenère.

En este nuevo artículo vamos a tratar el *método de la escítala*. Para ello nuestros alumnos han debido ver los contenidos del bloque de Números de la programación del último ciclo de Primaria o primer ciclo de ESO:

— Sistemas de numeración. Operaciones con naturales.
— Divisibilidad de los números naturales. Criterios de divisibilidad. Números primos y compuestos. Descomposición de un número en factores primos.

Para desarrollar dicho método en clase la propuesta didáctica es la siguiente:

— Introducción histórica.
— Paso de la tira escítala a la cuadrícula $(i \times j)$, con un número total de $(i \times j)$ letras en la tira. Divisores del número de total de letras: posibilidades de cuadrículas.
— Cifrado y descifrado de mensajes.

Duración: Una sesión de clase.

La escítala

Este método ya lo utilizaban en la antiguedad los griegos, en particular lo empleaban los espartanos para transmitir sus informaciones secretas. Plutarco en el tomo III de las *Vidas paralelas* hace referencia a este método. Plutarco de Queronea (Quereronea, c. 46 o 50; Delfos, c. 120) fue un historiador, biógrafo y filósofo moralista griego, al cual se le concedió la ciudadanía romana, por lo que pasó a ser conocido como Lucio Mestrio Plutarco. Nació durante el gobierno del emperador romano Claudio, y estudió filosofía, retórica y matemáticas en la academia de Atenas. Uno de sus maestros fue Amonio, al cual citó en alguna de sus obras.

En el tomo citado se describe en qué consistía el método, que a rasgos generales, consiste en cortar dos trozos de madera redondos y de similar diámetro. Para transcribir el mensaje, usaban una tira de papel y la enrollaban alrededor del trozo de madera, transcribiendo lo que querían comunicar, posteriormente lo desenrollaban y enviaban dicha tira de papel, de tal manera que tanto emisor como receptor tenían en su posesión el trozo de madera de similares dimensiones, para poder realizar el cifrado y descifrado de mensajes. Se suele denominar a dicha tira de papel como al trozo de madera, la *escítala*. He aquí un fragmento de dicho tomo:

> […] Lo de la escítala es en esta forma: cuando los Éforos mandan a alguno de comandante de la armada o de general, cortan dos trozos de madera redondos, y enteramente iguales en el diámetro y en el grueso, de manera que los cortes se correspondan perfectamente entre sí. De éstos guardan el uno, entregando el otro al nombrado, a estos trozos los llaman escítalas. Cuando quieren, pues, comunicar una cosa secreta e importante, forman una tira de papel, larga y estrecha como un listón, y la acomodan al trozo o escítala que guardan, sin que sobre ni falte, sino que ocupan exactamente con el papel todo el hueco; hecho esto, escriben en el papel lo que quieren, estando arrollado en la escítala. Luego que han escrito, quitan el papel, y sin el trozo de madera lo envían al general. Recibido por éste, nada puede sacar de unas letras que no tienen unión, sino que están cada una por su parte; pero tomando su escítala, extiende en ella la cortadura de papel, de modo que, formándose en orden el círculo, y

correspondiendo unas letras con otras, las segundas con las primeras, se presente todo lo escrito seguido a la vista. Llámase la tira escítala, igualmente que el trozo de madera, al modo que lo medido suele llevar el nombre de la medida […]

(Fragmento obtenido del texto: *Breve historia de la Criptografía Clásica* de José Luis Tábara)

Figura 1. La escítala (Wikimedia Commons)

Para entender cómo funcionaba en la práctica el método de la escítala, desarrollamos a continuación varios ejemplos tanto de cifrado como de descifrado de mensajes para trabajar con nuestros alumnos.

Para cifrar un determinado texto, se deben seguir los siguientes pasos:

1) Contar el número de letras que tiene dicho texto.
2) Obtener los divisores de dicho número.
3) Se pueden usar diferentes cuadrículas, en función de las posibilidades que den los divisores obtenidos en el paso anterior (filas × columnas).
4) Dibujar la cuadrícula (filas × columnas).
5) Escribir el texto en horizontal, empezando por la casilla que está más arriba y a la izquierda. Es decir, se deben ir rellenando filas.
6) El texto cifrado se obtiene al leer en vertical desde arriba hacia abajo empezando por la izquierda, es decir, de columna en columna.

Ejemplo 1: Vamos a cifrar el texto: «el taller de matemáticas»

1) 21 letras.
2) Divisores: 1, 3, 7, 21.
3) Cuadrícula: 3 × 7 o 7 × 3.
4) Por ejemplo, cuadrícula 3 × 7 (es decir, 3 filas y 7 columnas).
5) La cuadrícula con el texto nos queda:

e	l	t	a	l	l	e
r	d	e	m	a	t	e
m	a	t	i	c	a	s

6) El texto cifrado es:

E	R	M	L	D	A	T	E	T	A	M	I	L	A	C	L	T	A	E	E	S

Ejemplo 2: Cifrar el texto del ejemplo anterior pero ahora utilizando una cuadrícula de 7 × 3:

El texto cifrado es:

Si al contar el número de letras del texto se obtiene un número primo, es decir, el texto solo tiene por divisores el 1 y el propio número, es aconsejable añadir una letra (un espacio en blanco) para poder cifrar dicho texto ya que así se obtendrá un número compuesto que tendrá muchos más divisores.

Ejemplo 3: Cifrar el texto: «matemáticas»

1) Salen 11 letras, como es un número primo, añadimos un espacio en blanco (que lo indicaremos con un guión «–»), y así tenemos 12 letras en total.
2) Divisores; 1, 2, 3, 4, 6 y 12.
3) Posibilidades: 1×12, 2×6, 3×4, 12×1, 6×12, 4×3 (Es obvio que tanto 1×12 como 12×1 no se van a usar, ya que el texto quedaría tal cual).
4) Por ejemplo, usamos la cuadrícula 3×4 (3 filas y 4 columnas).
5) Dicha cuadrícula con el texto nos queda:

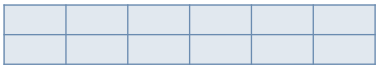
m	a	t	e
m	a	t	i
c	a	s	–

6) El texto cifrado es:

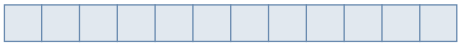
M	M	C	A	A	A	T	T	S	E	I	–

Probar ahora a cifrar dicho texto con otras cuadrículas:

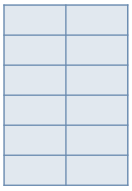
a) 2×6:



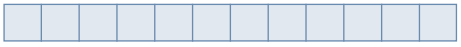
El texto cifrado es:



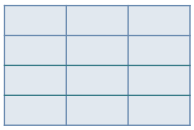
b) 6×2:



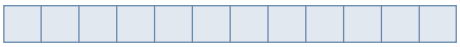
El texto cifrado es:



c) 4×3:



El texto cifrado es



Para descifrar un determinado texto, se deben seguir los siguientes pasos:

1) Contar el número de letras que tiene dicho texto.
2) Obtener los divisores de dicho número.
3) Se pueden usar diferentes cuadrículas, en función de las posibilidades que den los divisores obtenidos en el paso anterior (filas × columnas).
4) Dibujar la cuadrícula (filas × columnas).
5) Escribir el texto en vertical, empezando por la casilla que está más arriba y a la izquierda. Es decir, se debe ir rellenando columnas.
6) El texto descifrado se obtiene al leer en horizontal desde arriba empezando por la izquierda, es decir, de fila en fila.

Ejemplo 4: Ahora proponemos la realización de la operación inversa, es decir, descifrar el texto:

P	I	A	R	R	C	O	E	A	N	M	C	T	O	I	O	S	O	N	D	N	O	E	E	S	V	S

El texto descifrado es:

Conclusiones

La puesta en práctica en clase con nuestros alumnos es muy dinámica, ya que por un lado muestran interés por un tema que no lo han tratado en su clase habitual de matemáticas, y por otro porque ponen en práctica los contenidos que han visto y trabajado en su clase de matemáticas, como son los números naturales, sus divisores y sus múltiplos y números primos y números compuestos. Además, la presencia de otra persona diferente o ajena a sus maestros o profesores del día a día, también les sirve de motivación. Se suele aprovechar la semana matemática de los centros, y en concreto el programa de Conexión Matemática para desarrollar este tipo de actividades. También en la asignatura del Taller de Matemáticas.

En el próximo artículo de criptografía para principiantes veremos el *método de Della Porta*.

Referencias bibliográficas

Tábara, J. L. (s. f.) *Breve historia de la Criptografía Clásica*, descargada de la web Matemática Educativa. <http://www.matematicaeducativa.com/foro/download/file.php?id=1051>.

Escítala, (2020), en *Wikipedia*, recuperado el 23 de enero de 2021 de <https://es.wikipedia.org/wiki/Esc%C3%ADtala>.

Plutarco, (2021), en *Wikipedia*, recuperado el 23 de enero de 2021 de <https://es.wikipedia.org/wiki/Plutarco>.

Talleres de Conexión Matemática impartidos por el autor del presente artículo.

Enero de 2021
ISSN: 2386-8821e