Criptografía para principiantes: método Julio César y Vinegère

por
Óscar Carrión Lostal
(IES Valdespartera)

La *criptografía* (del griego κρύπτω krypto, *oculto*, y γράφω graphos, *escribir*, literalmente *escritura oculta*) es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y es empleada frecuentemente para permitir un intercambio de mensajes que solo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

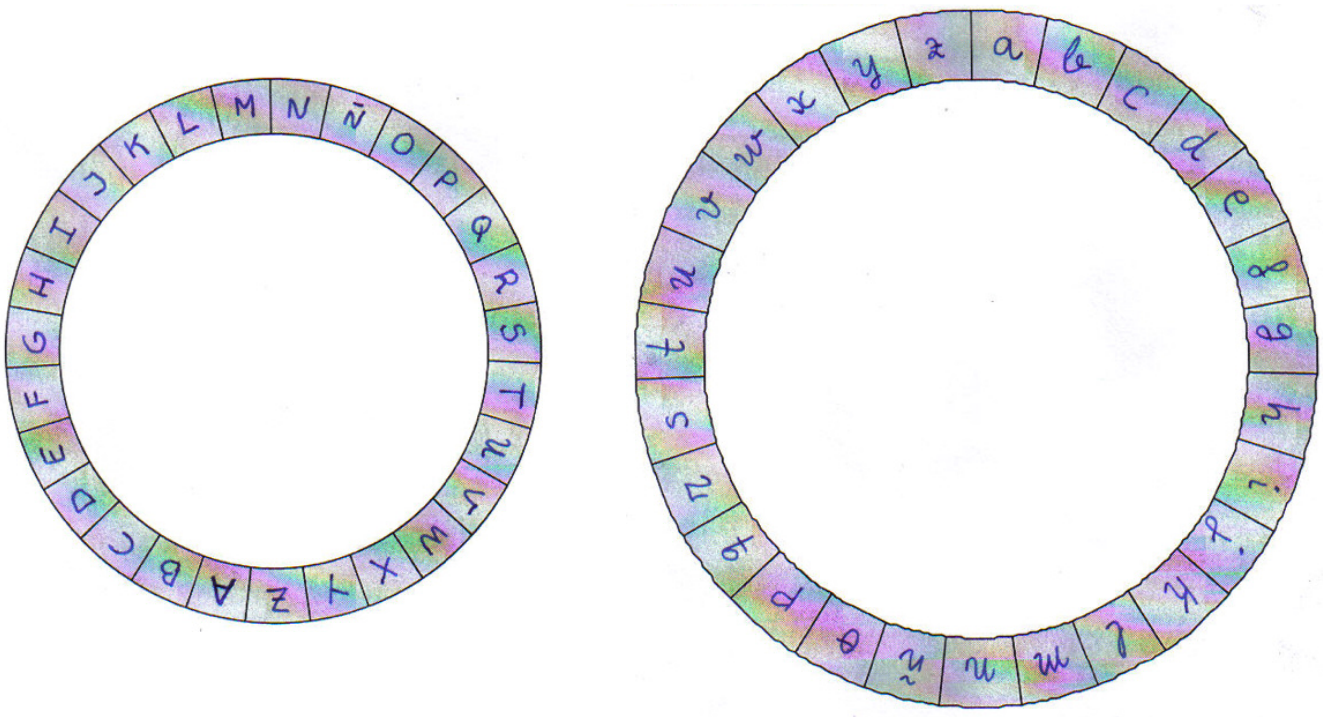
Con más precisión, cuando se habla de esta área de conocimiento como ciencia se debería hablar de *criptología*, que a su vez engloba tanto las técnicas de cifrado, es decir la criptografía propiamente dicha, como sus técnicas complementarias, entre las cuales se incluye el *criptoanálisis*, que estudia métodos empleados para romper textos cifrados con objeto de recuperar la información original en ausencia de las claves.

En este primer artículo sobre criptografía, vamos a ver distintos métodos de cifrar y descifrar mensajes, como el de Julio César y el de Vinegère.

Antes de entrar en materia, necesitamos que los alumnos se construyan su propia rueda para poder realizar las actividades propuestas de estos métodos de sustitución que vamos a proponer en este primer artículo.

Construye tu propia rueda

Se deben recortar las ruedas de la figura por el círculo exterior. En cada una se marca el centro del círculo y se introduce un pasador a través de ellos para poder deslizar una rueda sobre la otra. Hay que recordar, a lo largo de las diferentes actividades que se proponen a continuación, que el círculo con las letras en minúsculas corresponde con el texto a cifrar, y que el de las letras mayúsculas con el texto cifrado.



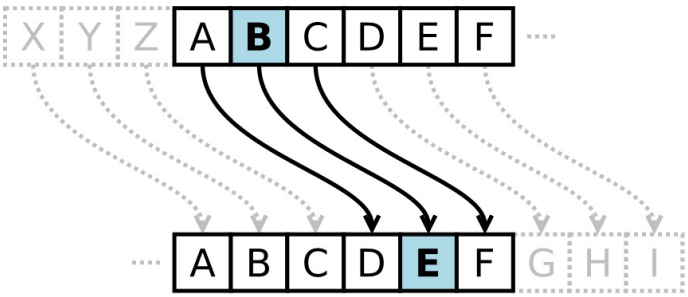
Ahora girando una de las ruedas se hace coincidir cada minúscula con su correspondiente mayúscula en las dos ruedas. Partiendo de la posición *a*−*A* se desplaza la rueda de dentro (en mayúsculas) hacia la izquierda tantos lugares como se desee (por ejemplo, cuando se desplaza tres lugares tenemos el cifrado de Julio César, que veremos a continuación).

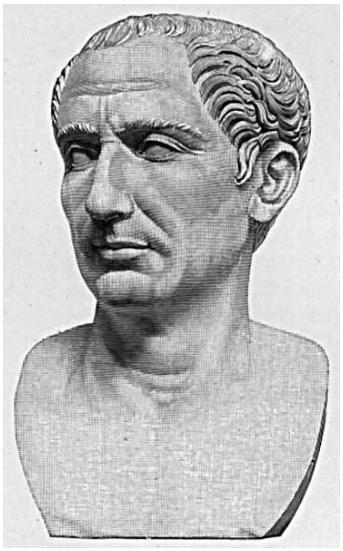
Las siguientes actividades están dirigidas para alumnos de último ciclo de Primaria o primer curso de ESO.

Julio César

Es un método de sustitución que consiste en cambiar cada letra del alfabeto por otra desplazada hacia delante varios lugares (en este caso tres) como queda reflejado en la siguiente tabla:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C





Así por ejemplo, para cifrar la palabra «matemáticas», haremos la sustitución teniendo en cuenta la tabla anterior o, lo que es equivalente, haciendo coincidir en la rueda construida la letra *a* con la letra *D*. En la siguiente tabla se obtiene el texto cifrado:

Texto descifrado	m	a	t	e	m	a	t	i	c	a	s
Texto cifrado	**O**	**D**	**W**	**H**	**O**	**D**	**W**	**L**	**F**	**D**	**V**

Como ejercicio podemos tratar de descifrar el texto MHURPLORCXULWD

Texto descifrado														
Texto cifrado	M	H	U	R	P	L	O	R	C	X	U	L	W	D

Este método de sustitución de Julio César tiene muchas variantes, ya que en vez de desplazar tres letras, podríamos haber desplazado otro número, y así obtener otro nuevo sistema de cifrado distinto. Podemos pedir a los alumnos que practiquen otros métodos de cifrado con sus compañeros, y que se propongan entre ellos palabras a descifrar…

Vinegère

Este método está basado en el método de Julio César haciendo uso además de una *palabra clave*. Para ayudarse a cifrar y descifrar textos con este método, se debe hacer uso de la rueda que se ha construido anteriormente.

Veamos un ejemplo: queremos cifrar el texto «matemáticas», usando el método de Vinegère y usando como palabra clave, por ejemplo, VINEGERE.

Si el texto a cifrar tiene más letras que la palabra clave, se debe repetir tantas veces como sea necesaria la palabra clave.

El procedimiento para cifrar dicho texto es: Nuestra primera letra a cifrar es la *m*, para ello utilizaré la primera letra de la palabra clave, que es la *V*, entonces debo hacer coincidir mi letra *a* minúscula (texto a cifrar) con la letra *V*, y ver qué letra le corresponde en la rueda a la *m*, que en nuestro caso es la *H*, y así sucesivamente.

Si nos dan una clave numérica, como 0123456789, significa lo siguiente: 0 que no desplazamos, es decir, la *a* coincide con la *A* en nuestra rueda, el 1 significa que desplazamos 1, por tanto en nuestra rueda pondremos la *a* con la *B*, el 2 significa desplazar dos lugares nuestra rueda, es decir hacer coincidir la *a* con la *C*, y así sucesivamente…

Texto descifrado	m	a	t	e	m	a	t	i	c	a	s
CLAVE	*V*	*I*	*N*	*E*	*G*	*E*	*R*	*E*	*V*	*I*	*N*
Texto cifrado	**H**	**I**	**G**	**I**	**R**	**E**	**L**	**M**	**X**	**I**	**F**

Ejemplo de ejercicios que podemos realizar con este método serían los siguientes:

1. Codificar el mensaje «taller de matemáticas» por el método de Vinegère usando la clave 0123456789:

Texto descifrado	t	a	l	l	e	r	d	e	m	a	t	e	m	a	t	i	c	a	s
CLAVE	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
Texto cifrado																			

2. Sabiendo que están cifrados por el método de Vinègere donde la clave es 0123456789, descifrar los siguientes mensajes:

Texto descifrado																				
CLAVE	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Texto cifrado	K	F	R	Ñ	I	W	J	L	L	D	J	P	N	D	W	P	K	F	M	B

Texto descifrado																				
CLAVE	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Texto cifrado	Q	V	G	U	M	L	K	T	M	T	M	P	X	L	P	N	K	T	B	X

Referencias

Criptografía (s.f.), en Wikipedia, recuperado el 28 de noviembre de 2020 de <https://es.wikipedia.org/wiki/Criptograf%C3%ADa>.