Si lo escondo, ¿lo encuentras?
Aritmética del reloj

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

El Cifrado de César

Cifrar consiste en convertir mensajes para que sólo los entienda la persona a quien va dirigido. Existen numerosas formas de hacer esto ya que los expertos van ideando nuevos métodos de cifrar y a su vez los criptoanalistas las van rompiendo.

Las matemáticas juegan un gran papel en estos métodos de cifrado ya que si se inventa un método sistemático (función de cifrado) será más fácil la traducción del texto original al texto cifrado. Si esta función de cifrado se puede expresar en términos matemáticos el trabajo que hay que hacer para cifrar o descifrar se simplifica. Actualmente se cuenta con ordenadores que nos permiten cifrar y descifrar de forma más rápida ya que todos los métodos algorítmicos son susceptibles de programar.

Uno de los métodos de cifrado más antiguo, que vamos a estudiar a continuación, es el Cifrado de César, llamado así en honor a Cayo Julio César, el líder militar y político que gobernó la República Romana. Se tiene documentación del uso de esta cifra con propósitos militares en *La guerra de las Galias* (siglo I aC)., donde se describe que César envió un mensaje a Cicerón en el que reemplaza las letras romanas por griegas. Más tarde (siglo II), Suetonio escribió *Vidas de los doce Césares* y describe el método de cifrado de César, algoritmo que consiste en el desplazamiento de tres espacios hacia la derecha de los caracteres del texto claro (se dice que la clave es 3).

1. Intenta cifrar la palabra **SECRETO** con este método. El mensaje cifrado es _____

No ha sido muy difícil puesto que el mensaje es muy corto. En mensajes más largos puede ser un poco más complicado. Para facilitar el trabajo nos podemos ayudar de una tabla en la que escribimos nuestro alfabeto en la primera fila y debajo un nuevo alfabeto pero desplazado 3 lugares (es decir empezando con d y acabando con c). Este alfabeto recibe el nombre de alfabeto de César (en honor a Julio César)

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

2. Cifrar usando el método de César el mensaje:

V	A	M	O	S		A	L		C	I	N	E

Ya sabes cifrar pero ahora vamos a resolver una serie de cuestiones relacionadas con este método:

3. ¿Es obligatorio desplazar siempre 3 lugares, es decir la clave siempre es 3?

A partir de ahora, al número seleccionado como clave lo llamamos *d*.

4. Cifrar usando el método de César, con clave $d=7$, el mensaje:

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

V	A	M	O	S		A	L		C	I	N	E

Cifrar usando el método de César, con clave d=11, el mensaje:

V	A	M	O	S		A	L		C	I	N	E

5. Si cambiamos la clave (el valor de desplazamiento), ¿te sirve la tabla anterior para cifrar? ¿Puedes usar algún material del maletín del espía para no tener que escribir esta tabla?

6. Para despistar a los "espías" decidimos usar diferentes claves cada día ¿Cuántas claves diferentes puedes seleccionar?

7. ¿Tiene sentido usar el valor d=0? ¿Y d=27? ¿Por qué?

8. ¿Eres capaz de escribir una expresión matemática que relaciona cada símbolo del mensaje original con el mensaje cifrado cuando se usa la clave d?

9. ¿Es obligatorio que el alfabeto de César esté ordenado? Si se admiten alfabetos desordenados ¿Cuántas claves diferentes existen?

10. ¿Cómo usar el disco para descifrar un mensaje?

11. Se ha cifrado con César: VRÑLGDULGDG ¿Qué dice el mensaje?

12. ¿Puede ser ANDXBBBBBBHKLJOP el criptograma de un mensaje en castellano, considerando sólo las 27 letras y cifrado por un método en el que cada símbolo del mensaje original se sustituye siempre por el mismo en el mensaje cifrado?

13. Nos fijamos en el cifrado ROT-13, (cifrado de César en el que la clave es 13, que coincide con la mitad de las 26 letras del alfabeto inglés en el que no existe la ñ). Este cifrado presenta una particularidad que vas a descubrir:

    ¿En que se convierte la letra A si se cifra mediante ROT-13?

    ¿Y la letra N?

    ¿Lo has averiguado? ¡Seguro que sí!: para descifrar un texto hay que hacer lo mismo que para cifrarlo. Esta sencillez para descifrar un mensaje fue la causa de que se usara este método. Por ejemplo comenzó a usarse en foros para escribir algo que solo se lea si se quiere, como soluciones de problemas y adivinanzas, y otros.

Para terminar esta actividad te vamos a proponer una variante del método de César:

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

Si lo escondo, ¿lo encuentras?
Aritmética del reloj

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

1. Vamos a usar una palabra que no tenga letras repetidas. Por ejemplo *clave*

2. Escribe en la tabla esta palabra y a continuación el resto de letras de nuestro abecedario. En nuestro ejemplo, el alfabeto será:

c	l	a	v	e	b	d	f	g	h	i	j	k	m	n	ñ	o	p	q	r	s	t	u	w	x	y	z

3. Escribe debajo el mismo alfabeto desplazado 3 lugares

c	l	a	v	e	b	d	f	g	h	i	j	k	m	n	ñ	o	p	q	r	s	t	u	w	x	y	z
v	e	b	d	f	g	h	i	j	k	m	n	ñ	o	p	q	r	s	t	u	w	x	y	z	c	l	a

4. Cifra el mensaje

V	A	M	O	S		A	L		C	I	N	E

Aparentemente el cifrado de César es poco seguro, pero en la época de Julio César no era de conocimiento general la idea de ocultar el significado de un texto mediante cifrado. En estos tiempos un mensaje cifrado con este método garantizaba la confidencialidad (la mayoría de la población era analfabeta).

Como dato curioso, más de 1500 años después, un cifrado similar al de César fue utilizado por la reina María Estuardo de Escocia, para conspirar junto con los españoles contra su prima Isabel I (en realidad, cayó en una trampa que organizaron agentes al servicio de Isabel I) Los mensajes cifrados de María los descifraron fácilmente los agentes de la reina usando análisis estadísticos, y quedó al descubierto la conspiración de la reina escocesa que perdió la cabeza en su ejecución el 8 de febrero de 1587.

A pesar de esto el cifrado César no quedó definitivamente descartado como método de cifrado seguro para los gobernantes del mundo: esta cifra también la usaron los oficiales sudistas en la Guerra de Secesión americana y por el ejército ruso en 1915.

Otro ejemplo, la policía italiana arresta en abril de 2006 al capo de la mafia siciliana Bernardo Provenzano que usaba el método de César para cifrar mensajes. Sus mensajes viajaban anotados en pequeños trozos de papel (conocidos como *pizzini* en dialecto siciliano). El método resultaba efectivo para un observador ocasional, pero evidentemente no para la policía, que conocía el sistema.

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