2 Divisibilidad

EN LA VIDA COTIDIANA... Criptografía y números primos

En este proyecto pretendemos que aprendas a:

- Reconocer la importancia de la criptografía y el criptoanálisis. • Utilizar el cifrado de César.
- Manejar el cifrado de César mejorado. • Utilizar los números primos en la criptografía.

1 La criptografía y el criptoanálisis

La criptografía es la ciencia que estudia la protección de la información con distintos métodos para impedir el acceso a la misma de personas no autorizadas.

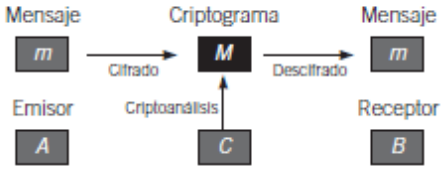
El criptoanálisis intenta averiguar los métodos anteriores para conseguir la información original.

La criptografía es tan antigua como la escritura. Se dice que las primeras civilizaciones que usaron la criptografía fueron la egipcia, la mesopotámica, la hindú y la china.

Hoy en día la criptografía es una disciplina de gran importancia: las comunicaciones de los gobiernos, entre las sedes de una empresa, en transacciones económicas, en el comercio por Internet, en las llamadas por teléfono móvil, necesitan estar protegidas para salvaguardar los intereses y la intimidad de las personas.

Los métodos criptográficos y de criptoanálisis actuales usan fórmulas muy complejas que aprovechan la enorme potencia de cálculo de los ordenadores.

El proceso suele ser el que ves en el gráfico. Un emisor *A* quiere mandar un mensaje *m* al receptor *B*. Para que un intruso *C* no pueda leerlo, *A* lo somete a un proceso de cifrado, consiguiendo un criptograma *M*, que es el que envía a *B*. Este, al recibirlo, lo somete a un proceso de descifrado, obteniendo el mensaje original, *m*. El criptoanálisis le serviría a *C*, si tiene éxito, para obtener el mensaje *m* a partir del criptograma *M*.



Vamos a estudiar a continuación uno de los métodos más famosos en la historia: el cifrado de César, creado por el gobernante romano Julio César.

2 El cifrado de César

El cifrado de César consiste en desplazar cada letra del alfabeto tres lugares. El texto que ciframos lo pondremos en minúscula y el criptograma obtenido en mayúsculas.

Observa la relación entre las letras:

a	b	c	d	e	f	g	h	i	j	k	l	m	n
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P

ñ	o	p	q	r	s	t	u	v	w	x	y	z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Por ejemplo, «enemigo» al cifrarlo queda HPHOLJR, y al descifrar ORUD obtenemos «mora». Compruébalo.

RESUELVE LAS SIGUIENTES ACTIVIDADES.

a) *Utilizando el cifrado de César, encripta estas frases.*
El examen es fácil. A las cinco en la plaza.

b) *Descifra el mensaje.*
HÑ HADOHP HV HÑ ÑXPHV

Una generalización sencilla de este método consiste en desplazar el alfabeto otro número distinto de 3 letras.

Así, si lo desplazamos 4 letras, entonces «enemigo» se traduce como IQIPMKS.

c) *Cifra las siguientes frases utilizando el cifrado de César generalizado según los desplazamientos* k *marcados para cada una de ellas.*

- k = *1. La bolsa subirá.*
- k = *2. Llegamos mañana.*

COMPETENCIA MATEMÁTICA

3 El cifrado de César mejorado

Una mejora del cifrado de César consiste en relacionar cada letra con otra, sin que haya un mismo desplazamiento para todas, eligiendo una combinación al azar. Este método se denomina sustitución monoalfabética.

Por ejemplo, si elegimos la relación:

a	b	c	d	e	f	g	h	i	j	k	l	m	n
B	W	E	R	T	Y	U	I	O	P	C	S	D	F

ñ	o	p	q	r	s	t	u	v	w	x	y	z
G	H	J	K	L	Z	X	A	V	Q	N	M	Ñ

la palabra «enemigo» sería TFTDOUH.

Este sistema es bastante seguro porque se pueden emplear unas 10^{28} relaciones distintas, tantas como reordenaciones del alfabeto se te ocurran, por lo que si alguien quisiera descifrar el texto, aunque conociera la técnica, no sabría qué reordenación se ha elegido.

REALIZA ESTAS ACTIVIDADES.

a) *Utilizando la relación estudiada, cifra estas frases.*
Vienen a las siete. Vende todo.

b) *Elige una reordenación del alfabeto y cifra las frases anteriores.*

A pesar de que este método parece muy seguro, basándonos en la frecuencia con que se repiten las letras en un idioma, y con la actual potencia de cálculo de los ordenadores, es posible descifrar los mensajes.

Date cuenta de que hasta ahora hemos visto métodos de cifrado y descifrado en los que tanto emisor como receptor conocen la forma de enviar y recibir mensajes, es decir, los métodos de cifrado y descifrado son comunes.

En la criptografía actual, sin embargo, no ocurre así: si queremos mandar un mensaje a alguien, sabremos cómo cifrarlo pero solamente el receptor sabrá cómo descifrarlo.

4 La utilidad de los números primos en criptografía

Los sistemas actuales de criptografía utilizan métodos numéricos muy complejos, con operaciones en las que se manejan números primos con gran cantidad de cifras.

Muchos matemáticos y científicos trabajan en métodos de cifrado y descifrado, y utilizan los números primos, ya que son la base ideal para un proceso de cifrado fácil y descifrado enormemente difícil.

Vamos a ver, a continuación, un método sencillo de cifrado en el que utilizaremos los números primos. Se requiere que tanto emisor como receptor conozcan cómo cifrar y descifrar mensajes.

A cada letra del alfabeto le haremos corresponder un número de dos cifras. La letra A la sustituiremos por 10, la B por 11 y así sucesivamente.

a/10	b/11	c/12	d/13	e/14	f/15	g/16
h/17	i/18	j/19	k/20	l/21	m/22	n/23
ñ/24	o/25	p/26	q/27	r/28	s/29	t/30
u/31	v/32	w/33	x/34	y/35	z/36	

El emisor aplica este método de cifrado: si el número correspondiente a la letra es primo, se deja como está, y si es compuesto, se le suma un número fijo, 30 en este caso.

a/40	b/11	c/42	d/13	e/44	f/45	g/46
h/17	i/48	j/19	k/50	l/51	m/52	n/23
ñ/54	o/55	p/56	q/57	r/58	s/29	t/60
u/31	v/62	w/63	x/64	y/65	z/66	

De este modo, la palabra «mates» sería 5240604429.

Para descifrar el mensaje hacemos grupos de dos cifras en los números y miramos la equivalencia en la tabla. Así, 17555140 29405840 descifrado es la frase «hola sara».

RESUELVE LAS ACTIVIDADES.

a) *Con el método anterior cifra estas frases.*
Ven mañana. Tengo frío.

b) *Descifra el texto.*
604844234429 573144 4429603113484058

c) *Inventa otro método para encriptar textos en el que utilices los números primos.*