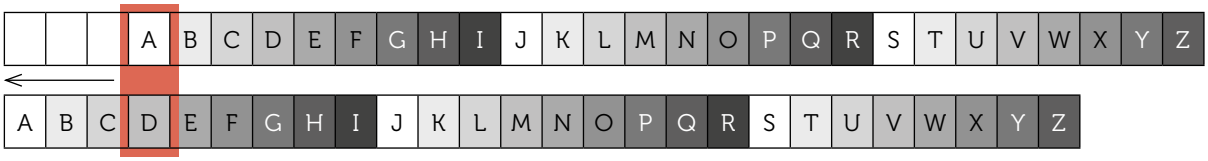
23 | Codificación
Criptología. El cifrado César

El cifrado César, también conocido como cifrado por desplazamiento, código de César o desplazamiento de César, es una de las técnicas de cifrado más simples y que más se ha usado a lo largo de la historia. Se trata de un tipo de cifrado por sustitución en el que cada letra del texto original es reemplazada por otra letra que se encuentra adelantada un número fijo de posiciones en el alfabeto. Por ejemplo, con un desplazamiento de 3, la letra A sería sustituida por la letra D, la letra B sería reemplazada por la letra E, etc. Este método de codificación debe su nombre a Julio César, quien lo usaba para comunicarse con sus generales.



» El cifrado César desplaza cada letra un determinado número de espacios en el alfabeto. En este ejemplo se utiliza un desplazamiento de tres espacios, de modo que una letra A en el texto original se convierte en una letra D en el texto codificado.

En muchas ocasiones el cifrado César forma parte de sistemas más complejos de codificación, como el cifrado Vigenère o, incluso, el sistema ROT13. Como todos los cifrados de sustitución alfabética simple, el cifrado César se descifra con facilidad, por lo que, en la práctica no protege las comunicaciones con demasiada seguridad.

Desde el punto de vista matemático, el cifrado César puede ser modelizado mediante una operación de suma en aritmética modular 26. Así, cada letra del alfabeto latino (de la A a la Z) queda identificada por un entero de 0 a 25. El texto plano se codifica introduciendo el desplazamiento de tres posiciones, es decir, sumando el valor de la clave (en este caso, 3). En consecuencia:

<letra encriptada> = (<letra plana> + clave)**mod**26

<letra plana> = (<letra encriptada> - clave)**mod**26

letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
código	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1 Codifica y decodifica el siguiente mensaje utilizando una clave de desplazamiento de valor 8:

Texto original: WIKIPEDIA, LA ENCICLOPEDIA LIBRE

Texto codificado:

2 Investiga la frecuencia de aparición de las diferentes letras en el idioma castellano. Selecciona un texto de muestra de no menos de 50 palabras y codifícalo con un cifrado César con clave de desplazamiento 12. Construye la tabla de frecuencias de aparición de las letras en el texto codificado y compáralo con la frecuencia teórica de los textos en castellano. Explica las conclusiones a las que llegas.

23 | Codificación
Criptología. El cifrado César

MATERIALES
Calculadora CASIO fx-570/991 SP X II Iberia

NIVEL EDUCATIVO
3º de ESO

ORIENTACIONES DIDÁCTICAS Y TÉCNICAS
- Se ha propuesto esta actividad para, además de tratar los contenidos curriculares correspondientes, analizar y valorar la importancia de los sistemas de codificación y encriptación.
- Para realizar las actividades, se hace uso de la funcionalidad *CALC*, que permite hallar el valor numérico de una expresión algebraica a partir del valor de las correspondientes variables. También se utiliza la función *Int*, a la que se accede mediante [ALPHA] [+]. Dicha función proporciona la parte entera de un número.

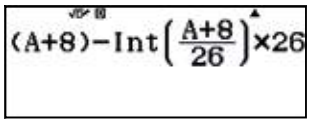
EJEMPLO DE SOLUCIÓN

1

Para codificar el mensaje utilizando una clave de desplazamiento de valor 8 hay que sumar 8 al valor numérico de cada letra, teniendo en cuenta que el máximo valor numérico que puede corresponder a una letra es 25, por lo que, una vez alcanzado este valor, se empieza a contar desde el cero.

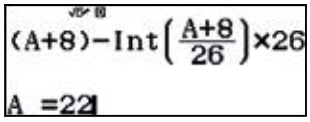
Se designa con A el valor numérico correspondiente a la letra en cuestión y se introduce la siguiente expresión:

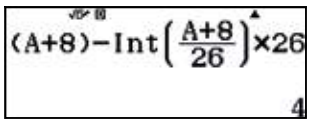
[(] [ALPHA] [(−)] [+] [8] [)] [−] [ALPHA] [+] [(] [ALPHA] [(−)] [+] [8] [)] [÷] [2] [6] [)] [×] [2] [6] [=]



Seguidamente se accede a la función *CALC* y se introducen los valores numéricos de las letras que forman el texto original:

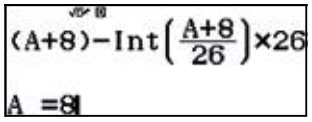
W – 22

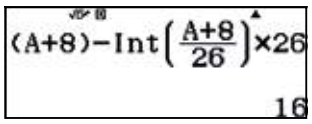




4 – E

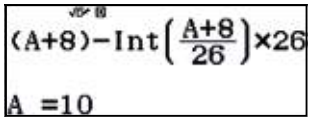
I – 8

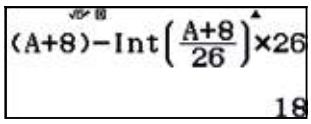




16 – Q

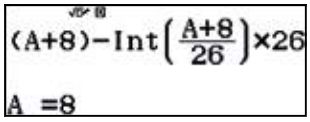
K – 10

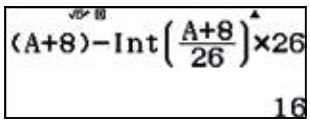




18 – S

I – 8





16 – Q

Procediendo análogamente con todas las letras se obtiene el mensaje codificado:

W	I	K	I	P	E	D	I	A		L	A		E	N	C	I	C	L	O	P	E	D	I	A		L	I	B	R	E
E	Q	S	Q	X	M	L	Q	I		T	I		M	V	K	Q	K	T	W	X	M	L	Q	I		T	Q	J	Z	M