Si ho amague, ho trobes?
Aritmètica del rellotge

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

El Xifratge de Cèsar

Xifrar consisteix en convertir missatges per a que només els entenga la persona a qui va adreçat. Existeixen nombroses formes de fer açò ja que els experts van ideant nous mètodes de xifrar i al seu torn els criptoanalistes les van trencant.

Les matemàtiques juguen un gran paper en aquests mètodes de xifratge ja que si s'inventa un mètode sistemàtic (funció de xifrat) serà més fàcil la traducció del text original al text xifrat. Si aquesta funció de xifrat es pot expressar en termes matemàtics el treball que cal fer per a xifrar o desxifrar se simplifica. Actualment es compta amb ordinadors que ens permeten xifrar i desxifrar de forma més ràpida posat que tots els mètodes algorítmics són susceptibles de programar.

Un dels mètodes de xifrat més antic, que anem a estudiar a continuació, és el Xifrat de Cèsar, anomenat així en honor a Gai Juli Cèsar, el líder militar i polític que va governar la República Romana. Es té documentació de l'ús de aquesta xifra amb propòsits militars en *La guerra de les Gàl·lies* (segle I aC)., on es descriu que Cèsar va enviar un missatge a Ciceró en el qual reemplaça les lletres romanes per gregues. Mes tard (segle II), Suetoni va escriure *Vides dels dotze Cèsars* i descriu el mètode de xifrat de Cèsar, algoritme que consisteix en el desplaçament de tres espais cap a la dreta dels caràcters del text clar (es diu que la clau és 3).

1. Intenta xifrar la paraula **SECRET** amb aquest mètode. El missatge xifrat és _____

No ha estat molt difícil posat que el missatge és molt curt. En missatges més llargs pot ser un poc més complicat. Per tal de facilitar el treball ens podem ajudar d'una taula en la qual escrivim el nostre alfabet en la primera fila i davall, en la segona fila, un nou alfabet però desplaçat 3 llocs (és a dir començant amb la lletra ç i acabant amb la c). Aquest alfabet rep el nom d'alfabet de Cèsar (en honor a Juli Cèsar)

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

2. Xifrar fent servir el mètode de Cèsar el missatge:

A	N	E	M		A	L		C	I	N	E	M	A

Ja saps xifrar però ara anem a resoldre una sèrie de qüestions relacionades amb aquest mètode:

3. És obligatori desplaçar sempre 3 llocs, és a dir la clau sempre és 3?

A partir d'ara, al número seleccionat com a clau l'anomenarem *d*.

4. Xifrar fent servir el mètode de Cèsar, amb clau *d*=7, el missatge:

A	N	E	M		A	L		C	I	N	E	M	A

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

Si ho amague, ho trobes?
Aritmètica del rellotge

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

Xifrar usant el mètode de Cèsar, amb clau *d*=11, el missatge:

A	N	E	M		A	L		C	I	N	E	M	A

5. Si canviem la clau (el valor de desplaçament), et serveix la taula anterior per a xifrar? Pots utilitzar algun material del maletí de l'espia per no haver d'escriure aquesta taula?

6. Per despistar als "espies" decidim fer servir diferents claus cada dia. Quantes claus diferents pots seleccionar?

7. Té sentit usar el valor *d*=0? I *d*=27? Per què?

8. Eres capaç d'escriure una expressió matemàtica que relacione cada símbol del missatge original amb el missatge xifrat quan s'usa la clau *d*?

9. És obligatori que l'alfabet de Cèsar estiga ordenat? Si s'admeten alfabets desordenats, quantes claus diferents existeixen?

10. Com utilitzar el disc per tal de desxifrar un missatge?

11. S'ha xifrat amb Cèsar: VROLGÇULWÇW Què diu el missatge?

12. Pot ser ANDXBBBBBBHKLJOP el criptograma d'un missatge en català, considerant només les 27 lletres i xifrat per un mètode on cada símbol del missatge original se substitueix sempre pel mateix en el missatge xifrat?

13. Ens fixem en el xifrat ROT-13, (xifrat de Cèsar de clau 13, coincideix amb la meitat de les 26 lletres de l'alfabet anglès en el qual no existeix la ç). Aquest xifrat presenta una particularitat que vas a descobrir:

    En què es converteix la lletra A si es xifra mitjançant ROT-13?

    ¿I la lletra N?

    Ho has esbrinat? Segur que sí!: per a desxifrar un text cal fer el mateix que per a xifrar-lo. Aquesta senzillesa per desxifrar un missatge fou la causa de que s'utilitzés aquest mètode. Per exemple es va començar a utilitzar en fòrums per escriure quelcom que només es puga llegir si es vol, com ara solucions de problemes i endevinalles, i altres.

Per acabar aquesta activitat anem a proposar-te una variant del mètode de Cèsar:

1. Anem a utilitzar una paraula amb totes les lletres diferents. Per exemple *clau*

2. Escriu en la taula aquesta paraula y a continuació la resta de lletres del nostre abecedari. En el nostre exemple, l'alfabet serà:

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

3. Escriu davall el mateix alfabet desplaçat 3 llocs

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

Si ho amague, ho trobes?
Aritmètica del rellotge

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

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

4. Xifra el missatge:

A	N	E	M		A	L		C	I	N	E	M	A

Aparentment el xifrat de Cèsar és poc segur, però en l'època de Juli Cèsar no era de coneixement general la idea d'ocultar el significat d'un text mitjançant xifrat. En aquests temps un missatge xifrat amb aquest mètode garantia la confidencialitat (la majoria de la població era analfabeta).

Com a dada curiosa, més de 1500 anys després, un xifrat semblant al de Cèsar fou utilitzat per la reina Maria Estuard d'Escòcia, per tal de conspirar junt amb els espanyols contra la seva cosina Isabel I (en realitat, va caure en una trampa que van organitzar agents al servei de Isabel I) Els missatges xifrats de Maria els van desxifrar fàcilment els agents de la reina fent servir anàlisis estadístics, i va quedar en descobert la conspiració de la reina escocesa que va perdre el cap en la seva execució el 8 de febrer de 1587.

Malgrat açò, el xifrat Cèsar no va quedar definitivament descartat com a mètode de xifrat segur per als governants del món: aquesta xifra també la van utilitzar els oficials sudistes en la Guerra de Secessió americana i l'exèrcit rus en 1915.

Una altre exemple, la policia italiana arresta en abril de 2006 al capo de la màfia siciliana Bernardo Provenzano que feia servir el mètode de Cèsar per a xifrar missatges. Els seus missatges viatjaven anotats en petits trossos de paper (coneguts com *pizzini* en dialecte sicilià). El mètode resultava efectiu per a un observador ocasional, però evidentment no per a la policia, que coneixia 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