

INDES- XIFRA- BLE

LES MATEMÀTIQUES AL SERVEI
DELS CODIS SECRETS

Aquest dossier pedagògic ha estat creat com a material complementari de l'obra de teatre **INDESXIFRABLE**, amb la voluntat d'apropar als alumnes el fascinant món de la criptografia d'una manera lúdica, participativa i adaptada a l'etapa de primària.

DOSSIER PEDAGÒGIC



AIXÒ ÉS UNA
CO-PRODUCCIÓ DE


ENIGMATITIS





INDESXIFRABLE

LES MATEMÀTIQUES AL SERVEI DELS CODIS SECRETS

L'objectiu principal del dossier és que els alumnes experimentin en primera persona alguns dels sistemes de xifrar i desxifrar que es mencionen durant l'espectacle. A través de reptes criptogràfics on podran descobrir que darrere dels missatges secrets s'hi amaguen matemàtiques, llengua, història... i molta imaginació!

I si encara no heu vist l'obra? No patiu gens ni mica!

Totes les activitats del dossier van acompanyades d'explicacions clares i entenedores, pensades perquè mestres i alumnes pugueu treballar-les de manera autònoma a l'aula. D'aquesta manera, tant si heu vist l'espectacle com si encara no, podreu endinsar-vos junts en el joc d'escriure i llegir missatges secrets.

Al llarg del dossier, els alumnes es convertiran en aprenents d'espia i posaran a prova diferents tècniques de criptografia, com ara:

- Xifrat per transposició
- Xifrat monoalfabètic
- Xifrat polialfabètic

Aprendre història tot jugant

Les activitats també permeten contextualitzar la criptografia dins la història, mostrant com la necessitat de comunicar missatges secrets ha acompanyat la humanitat des de fa segles. Els alumnes descobriran que xifrar informació no és pas una idea moderna!

I si voleu anar encara més enllà...

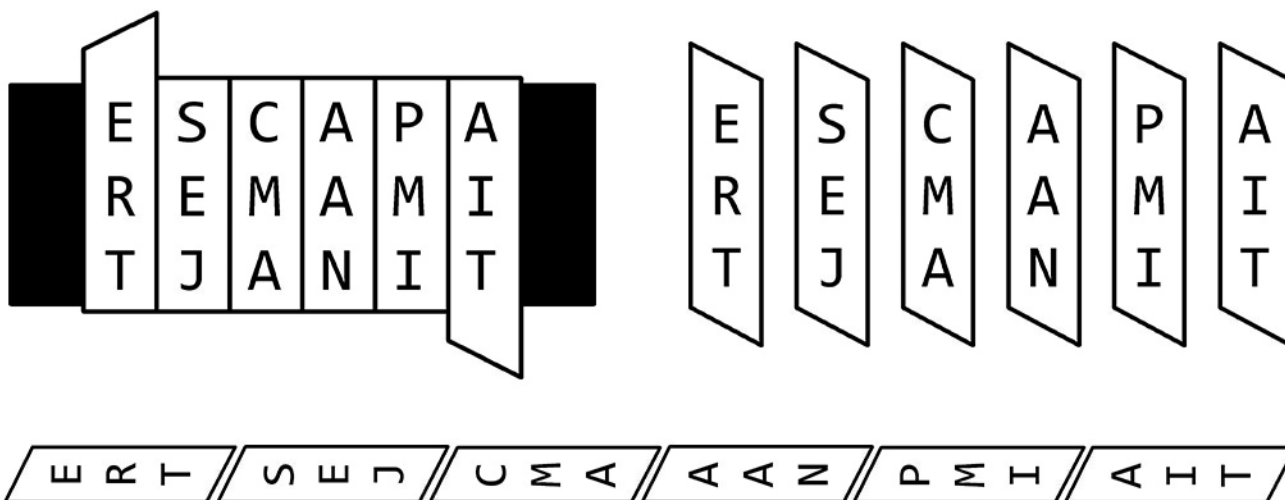
Us convidem a venir a veure l'obra INDESXIFRABLE, on els alumnes viuran aquest viatge a través del temps d'una manera divertida i sorprenent.

Acompanyaran els protagonistes des dels valents espartans de l'antiga Grècia, passant per inventors i estratèges, fins a arribar als misteriosos hackers del segle XXI.

Prepareu el llapis, el paper i la curiositat... perquè no tot el que es llegeix s'entén a la primera!

1. XIFRAT DE TRANSPOSICIÓ “L’escícala espartana”

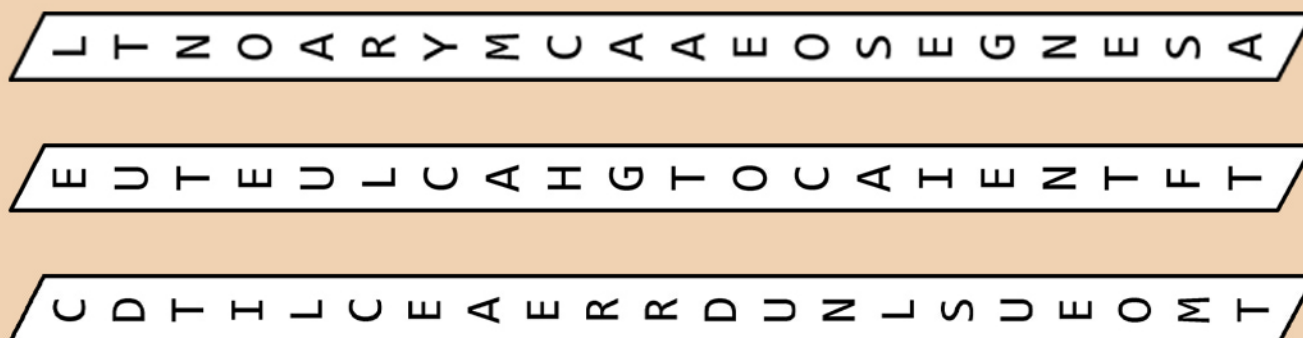
Tal i com ens ha explicat en GARBO, els grecs van inventar aquest curiós mètode de xifrat. Enrotllaven una tira de cuir sobre un pal de fusta i escrivién un missatge horitzontalment tot girant el pal per tal d’emplenar tot el cuir amb el text.



En acabat, desenrotllaven la tira de cuir i el missatge quedava completament il·legible. Per tal de recuperar el missatge calia enrotllar novament la tira de cuir en un pal que tingués el mateix **DIÀMETRE** que el pal original.

JOC 1

A l'exemple anterior el text està dividit en tres files, però també podia estar dividit en quatre, cinc... Seràs capaç de desxifrar els següents missatges?





LES MATEMÀTIQUES AL SERVEI DELS CODIS SECRETS

2. XIFRAT DE SUBSTITUCIÓ MONOALFABÈTICA “Juli Cèsar”

Sembla ser que Juli Cèsar va inventar aquest mètode per comunicar-se de forma secreta. Va utilitzar dues vares de fusta on previament hi havia escrit un alfabet al damunt de cadascuna. Aleshores, per xifrar un missatge, bellugava una fusta respecte l'altra. En l'exemple hem bellugat la fusta inferior dos espais cap a l'esquerra de tal manera que la paraula CÈSAR esdevé EGUCT



CÈSAR = **EGUCT**

Per desxifrar un text d'aquest tipus cal fer un breu anàlisi de freqüència per tal de descobrir quina lletra apareix més sovint en el text. Habitualment les lletres més freqüents són la E i la A. D'aquesta manera podem intentar trobar articles com EL o LA, el pronom QUE o aquelles paraules que ens ajudin a desxifrar la resta del missatge.

JOC 2

Un cop sabem com abordar un text xifrat d'aquest tipus, creus que seràs capaç de desxifrar aquests dos textos?

**TVIJIVIMBS WIV STXMQMWXE M BMQTPI UYI
TIWWMQMWXE M XIRMV VES - EPFIVX IMRWXIMR**

**ZP LSZ LZZLYZ OBTHUZ APUNBLZZPT KVZ JLYCLSSZ
MHYPLT LS KVISL KL IHQHUHKLZ - DVVKF HSSLU**



LES MATEMÀTIQUES AL SERVEI DELS CODIS SECRETS

3. XIFRAT DE SUBSTITUCIÓ POLIALFABÈTICA “Blaise de Vigenère”

El següent mètode data del segle XVI. En Blaise de Vigenère va ser un diplomàtic francès que inventà aquest interessant mètode de xifrat, inspirat en el mètode de Juli Cèsar però substituïnt les lletres de l'alfabet no només per un altre alfabet sinó per 26 alfabets diferents. A més, per xifrar un missatge cal l'intervenció d'una contrassenya. Veiem un exemple:

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



LES MATEMÀTIQUES AL SERVEI DELS CODIS SECRETS

Missatge a xifrar: **B L A I S E D E V I G E N E R E**

Contrassenya: **P A R I S**

Per xifrar el missatge cal fer coincidir la contrassenya amb el missatge tantes vegades com calgui. Ara buscarem per coordenades la lletra xifrada, cercant la lletra del missatge en l'eix d'ordenades i la que li correspongui de la contrassenya en l'eix de les abscises:

B	L	A	I	S	E	D	E	V	I	G	E	N	E	R	E
P	A	R	I	S	P	A	R	I	S	P	A	R	I	S	P
Q	L	R	Q	K	T	D	V	D	A	V	E	E	M	J	T

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



LES MATEMÀTIQUES AL SERVEI DELS CODIS SECRETS

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

JOC 3

Amb l'ajuda del quadre de Vigenère, seràs capaç de desxifrar els següents missatges? Tingues en compte que el procés de desxifrat no és com el de xifrat. Caldrà que pensis una mica abans d'abordar els missatges.

Missatge 1:

KCFHFA BOK FQSLZFAI GQR VGBIR

Contrassenya:

ROMA

Missatge 2:

PAUBDECME BAB PT VBFRPZ LSSN

Contrassenya:

LISBOA

Missatge 3:

TS VGMJWXTUF SDU NDSK OCEGSVAQG

Contrassenya:

MOSCU