Actividad 01. Cifrados básicos

1. Uso de Escítala

Usa algún instrumento de la clase que te sirva de bastón, puede ser un lápiz, pata de la silla, de la mesa, un bolígrafo, … Enrolla un papel alrededor del instrumento utilizado como bastón y escribe un mensaje a transmitir.
Dale el texto a otro compañero y comprueba que es capaz de descifrar el mensaje.
Comprueba también que si cae en manos del enemigo no es capaz de descifrarlo.

Realizado en clase.

2. Cifrador de Polibyos

Envía a un compañero un mensaje cifrado mediante el cifrador de Polibyos.
El mensaje deberá incluir una pregunta que el compañero deberá contestarle. Así podrás comprobar si el proceso ha funcionado correctamente.

	1	2	3	4	5	6
1	a	b	c	d	e	f
2	g	h	i	j	k	l
3	m	n	ñ	o	p	q
4	r	s	t	u	v	w
5	x	y	z	.	,	(
6	)		"	-	+	*

MENSAJE ORIGINAL
en que dia estamos

MENSAJE CIFRADO
153262364415621423116215424311 3134

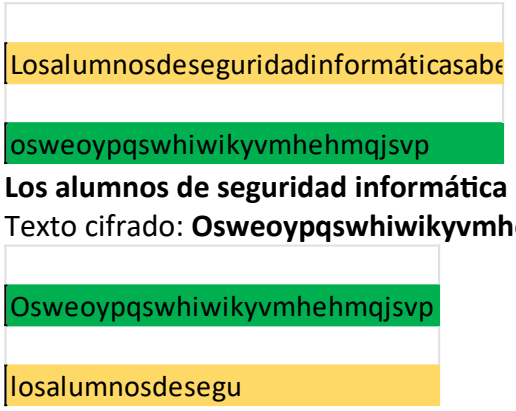
MENSAJE CIFRADO
153262364415621423116215424311 3134

MENSAJE ORIGINAL
en que dia estamo

Mensaje: en que dia estamos
Mensaje cifrado: **153262364415621423116215424311 3134**
Mensaje descifrado: en que día estamo
Respuesta: Lunes

3. Cifrado de César

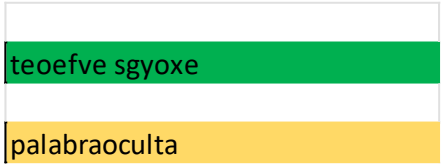
Cifra mediante el cifrado de César, desplazamiento 4, el siguiente mensaje:



Los alumnos de seguridad informática saben cifrar información

Texto cifrado: **Osweoypqswhiwikyvmhehmqjsvp**

Descifra mediante el cifrado de César el siguiente mensaje:



Texto cifrado: **teoefve sgyoxe**

Texto descifrado: **palabraoculta**

Nota. Los espacios en blanco no los cifres ni descifres.

4. Cifrado de Vigénere

Teniendo la tabla de cifrado de Vigénere siguiente:

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

Estableciendo como clave: “HELADO”:

5. Cifra el siguiente texto:

REINICIA EL EQUIPO

Texto cifrado: YISNLQOEOLHFBMAO

Texto en claro	reinicia el equipo		R	E	I	N	I	C	I	A		E	L		E	Q	U	I	P	O
CLAVE	helado		H	E	L	A	D	O	H	E		L	A		D	O	H	E	L	A
			Y	I	S	N	L	Q	O	E		O	L		H	F	B	M	A	O

6. Descifra el siguiente texto:

ZMDTHAH SAEUAAMGO ÑWTYI MLBA

Texto descifrado: SISTEMA OPERATIVO LINUX MINT

Texto en claro	SISTEMA OPERATIVO LINUX MINT	S I S T E M A O P E R A T I V O L I N U X M I N T
CLAVE	HELADO	H E L A D O H E L A D O H E L A D O H E L A D O H

	ZMDTHAH
Texto	SAEUAAMGO
cifrado	ÑWTYI MLBA

Z M D T H A H S A E U A A M G O Ñ W T Y I M L B A

Nota. Los espacios en blanco no los cifres ni descifres.

5. Cifrado de Vernam

Aplica cifrado Vernam y muestra el texto cifrado:

Texto a cifrar: **cosa**

Palabra	cosa	c	o	s	a
	Código ASCII	99	111	115	97
	Binario	01100011	01101111	01110011	01100001

CLAVE	948/	9	4	8	/
	Código ASCII	57	52	56	47
	Binario	00111001	00110100	00111000	00101111

Palabra	01100011	01101111	01110011	01100001
CLAVE	00111001	00110100	00111000	00101111
XOR	01011010	01011011	01001011	01001110

CIFRADO Z[KN	Z	[	K	N

Texto a cifrar: **hola**

Palabra	hola	h	o	l	a
	Código ASCII	104	111	108	97
	Binario	01101000	01101111	01101100	01100001

CLAVE	948/	9	4	8	/
	Código ASCII	57	52	56	47
	Binario	00111001	00110100	00111000	00101111

Palabra	01101000	01101111	01101100	01100001
CLAVE	00111001	00110100	00111000	00101111
XOR	01010001	01011011	01010100	01001110

CIFRADO Q[TN	Q	[	T	N