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	MENSAJE ORIGINAL							
1	а	b	С	d	е	f	en que dia estamos							
2	g	h	i	j	k	ı								
3	m	n	ñ	0	р	q	MENSAJE CIFRADO							
4	r	s	t	u	٧	w	1532623644156214231162154243113134							
5	х	у	z		,	(
6)		"	-	+	*								
							MENSAJE CIFRADO							
							1532623644156214231162154243113134							
							MENSAJE ORIGINAL							
							en que dia estamo							

Mensaje: en que dia estamos

Mensaje cifrado: 1532623644156214231162154243113134

Mensaje descifrado: en que día estamo

Respuesta: Lunes

3. Cifrado de César

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

Losalumnos de segurida dinformáticas abe

osweoypqswhiwikyvmhehmqjsvp

Los alumnos de seguridad informática saben cifrar información

Texto cifrado: Osweoypqswhiwikyvmhehmqjsvp

Osweoypqswhiwikyvmhehmqjsvp

losalumnosdesegu

Descifra mediante el cifrado de César el siguiente mensaje:

teoefve sgyoxe

palabraoculta

Texto cifrado: **teoefve sgyoxe** Texto descifrado: **palabraoculta**

palabraoculta

teoefvesgyoxe

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

4. Cifrado de Vigénere

Teniendo la tabla de cifrado de Vigénere siguiente:

												`				<u> </u>											
	Α	В	С	D	Е	F	G	Н	1	J	K	L	М	N	Ñ	О	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z
Α	Α	В	С	D	Е	F	G	Н	I	J	K	L	М	N	Ñ	О	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z
В	В	С	D	Е	F	G	Н	ı	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α
С	С	D	E	F	G	Н	ı	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В
D	D	E	F	G	Н	ı	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В	С
E	E	F	G	Н	1	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В	С	D
F	F	G	Н	Ι	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В	С	D	E
G	G	Н	I	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	V	w	Х	Υ	Z	Α	В	С	D	E	F
Н	Н	I	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	V	w	Х	Υ	Z	Α	В	С	D	Е	F	G
1	ı	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	w	х	Υ	Z	Α	В	С	D	E	F	G	Н
J	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	W	х	Υ	Z	Α	В	С	D	E	F	G	Н	Ι
K	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	V	w	Х	Υ	z	Α	В	С	D	E	F	G	Н	ı	J
L	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	w	х	Υ	Z	Α	В	С	D	E	F	G	Н	Ι	J	K
М	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	w	х	Υ	Z	Α	В	С	D	E	F	G	Н	I	J	K	L
N	N	Ñ	0	Р	Q	R	S	Т	U	٧	W	х	Υ	Z	Α	В	С	D	E	F	G	Н	I	J	K	L	М
Ñ	Ñ	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В	С	D	Е	F	G	Н	ı	J	K	L	М	N
0	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В	С	D	Е	F	G	Н	ı	J	K	L	М	N	Ñ
Р	Р	Q	R	S	Т	U	V	w	Х	Υ	Z	Α	В	С	D	Е	F	G	Н	I	J	K	L	М	N	Ñ	0
Q	Q	R	S	Т	U	٧	w	Х	Υ	Z	Α	В	С	D	E	F	G	Н	ı	J	K	L	М	N	Ñ	0	Р
R	R	S	Т	U	V	w	Х	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J	K	L	М	N	Ñ	О	Р	Q
S	S	Т	U	٧	w	Х	Υ	Z	Α	В	С	D	Е	F	G	Н	ı	J	K	L	М	N	Ñ	0	Р	Q	R
Т	Т	U	٧	W	х	Υ	Z	Α	В	С	D	E	F	G	Н	1	J	K	L	М	N	Ñ	0	Р	Q	R	S
U	U	٧	W	Х	Υ	Z	Α	В	С	D	E	F	G	Н	ı	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т
٧	٧	W	Х	Υ	Z	Α	В	С	D	E	F	G	Н	_	J	K	L	М	Ν	Ñ	0	Р	Q	R	S	Т	U
W	W	Х	Υ	Z	Α	В	С	D	E	F	G	Н	1	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧
Х	Х	Υ	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	N	Ñ	0	Р	Q	R	S	т	U	V	W
Υ	Υ	Z	Α	В	С	D	Е	F	G	Н	ı	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	W	Х
Z	Z	Α	В	С	D	Ε	F	G	Н	-	J	K	L	М	N	Ñ	0	Р	Q	R	S	Т	U	٧	w	Х	Υ

Estableciendo como clave: "HELADO":

5. Cifra el siguiente texto:

REINICIA EL EQUIPO

Texto cifrado: YISNLQOEOLHFBMAO

Texto en claro	reinicia el equipo	R	Ε	L	N	L	С	I	Α	Ε	L	Ε	Q	U	I	Р	0
CLAVE	helado	Н	E	L	Α	D	0	Н	Е	L	Α	D	0	Н	Ε	L	Α
		Υ	I	S	N	L	Q	0	Ε	0	L	Н	F	В	М	Α	0

6. Descifra el siguiente texto:

ZMDTHAH SAEUAAMGO ÑWTYI MLBA

Texto descifrado: SISTEMA OPERATIVO LINUX MINT

Texto SISTEMA

en OPERATIVO LINUX

CLAVE HELADO HELADOHELA DOHEL ADOH

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

cosa						
CUSa	С	0	S	а		
Código						
ASCII	99	111	115	97		
Binario	01100011	01101111	01110011	01100001		
948/	9	4	8	/		
Código						
ASCII	57	52	56	47		
Binario	00111001	00110100	00111000	00101111		
abra	01100011	01101111	01110011	01100001		
AVE	00111001	00110100	00111000	00101111		
OR	01011010	01011011	01001011	01001110		
Z[KN	Z	[K	N		
	ASCII Binario 948/ Código ASCII Binario abra AVE OR	ASCII 99 Binario 01100011 948/ 9 Código ASCII 57 Binario 00111001 abra 01100011 AVE 00111001 OR 01011010	ASCII 99 111 Binario 01100011 01101111 948/ 9 4 Código ASCII 57 52 Binario 00111001 00110100 abra 01100011 01101111 AVE 00111001 00110100 OR 01011010 01011011	ASCII 99 111 115 Binario 01100011 01101111 01110011 948/ 9 4 8 Código ASCII 57 52 56 Binario 00111001 00110100 00111000 abra 01100011 01101111 01110011 AVE 00111001 0011010 00111100 OR 01011010 01011011 01001011		

Texto a cifrar: hola

Texto a cifra	r: hola				
Palabra	hola	h	0	I	а
	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
Pa	labra	01101000	01101111	01101100	01100001
CL	.AVE	00111001	00110100	00111000	00101111
Х	OR	01010001	01011011	01010100	01001110
CIFRADO	Q[TN	Q	[Т	N