Actividad 01. Cifrados básicos

- 1. Uso de Escítala
- 2. Cifrador de Polybios
- 3. Cifrado de César
- 4. Cifrado de Vigenère
- 5. Cifra el siguiente texto:
- 6. Descifra el siguiente texto:
- 7. Cifrado de Vernam

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.

EJERCICIO REALIZADO YA EN CLASE.

2. Cifrador de Polybios

Envía a un compañero un mensaje cifrado mediante el cifrador de Polybios. 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				MENS	AJE OR	IGINAL								
	1	а	b	С	d	е	f				esto	es un e	jemplo								
	2	g	h	i	j	k	1														
	3	m	n	ñ	0	р	q				MENS	SAJE CI	FRADO								
	4	r	s	t	u	٧	w		1542433462154262443262152415313526												
	5	х	у	z		,	(
	6)		"	-	+	*														
													FRADO								
									26	523121	5414311	114623	46231441	54143	15						
											MENS	AJE OR	IGINAL								
												tad o n									
>	Hoja1	Hoja2		+																	

El mensaje es: "esto es un ejemplo", y el mensaje cifrado es: "1542433462154262443262152415313526".

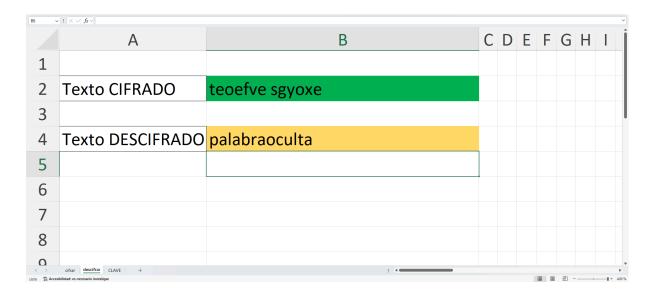
El mensaje cifrado es: "2623121541431114623462314415414315" y el mensaje es: "*libertad o muerte*".

3. Cifrado de César

Cifra mediante el cifrado de César, desplazamiento 4, el siguiente mensaje: Los alumnos de seguridad informática saben cifrar información

Descifra mediante el cifrado de César el siguiente mensaje: teoefve sgyoxe

Nota. Los espacios en blanco no se cifran ni se descifran.



El texto descifrado es: "palabraoculta"

4. Cifrado de Vigenère

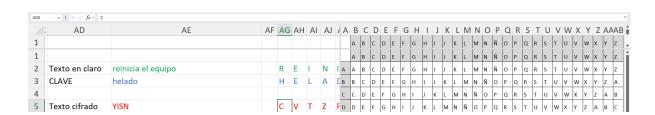
Teniendo la tabla de cifrado de Vigenère siguiente, establece como clave: "HELADO":



La palabra clave "HELADO" tiene como texto descifrado "LINUX MINT".

5. Cifra el siguiente texto:

REINICIA EL EQUIPO



El texto "REINICIA EL EQUIPO" tiene como palabra clave "helado" y texto cifrado "YSIN".

6. Descifra el siguiente texto:

ZMDTHAH SAEUAAMGO ÑWTYI MLBA

Nota. Los espacios en blanco no se cifran ni se descifran.

Jorge Escobar Viñuales 43835997K Seguridad Informática



La frase "ZMDTHAH SAEUAAMGO ÑWTYI MLBA" con clave "HELADO", su texto descifrado es "SISTEMA OPERATIVO LINUX MINT".

7. Cifrado de Vernam

Aplica cifrado Vernam y muestra el texto cifrado:

	А	В	С	Е	G	I		
1	Palabra	cosa	С	0	S	а		
2		Código ASCII	99	111	115	97		
3		Binario	01100011	01101111	01110011	01100001		
12								
13	CLAVE	948/	9	4	8	/		
14		Código ASCII	57	52	56	47		
15		Binario	00111001	00110100	00111000	00101111		
28								
29	Pala	abra	01100011	01101111	01110011	01100001		
30	CLA	AVE	00111001	00110100	00111000	00101111		
39	X	OR	01011010	01011011	01001011	01001110		
40								
41	CIFRADO	Z[KN	Z	[K	N		

La palabra "cosa" tiene este cifrado.