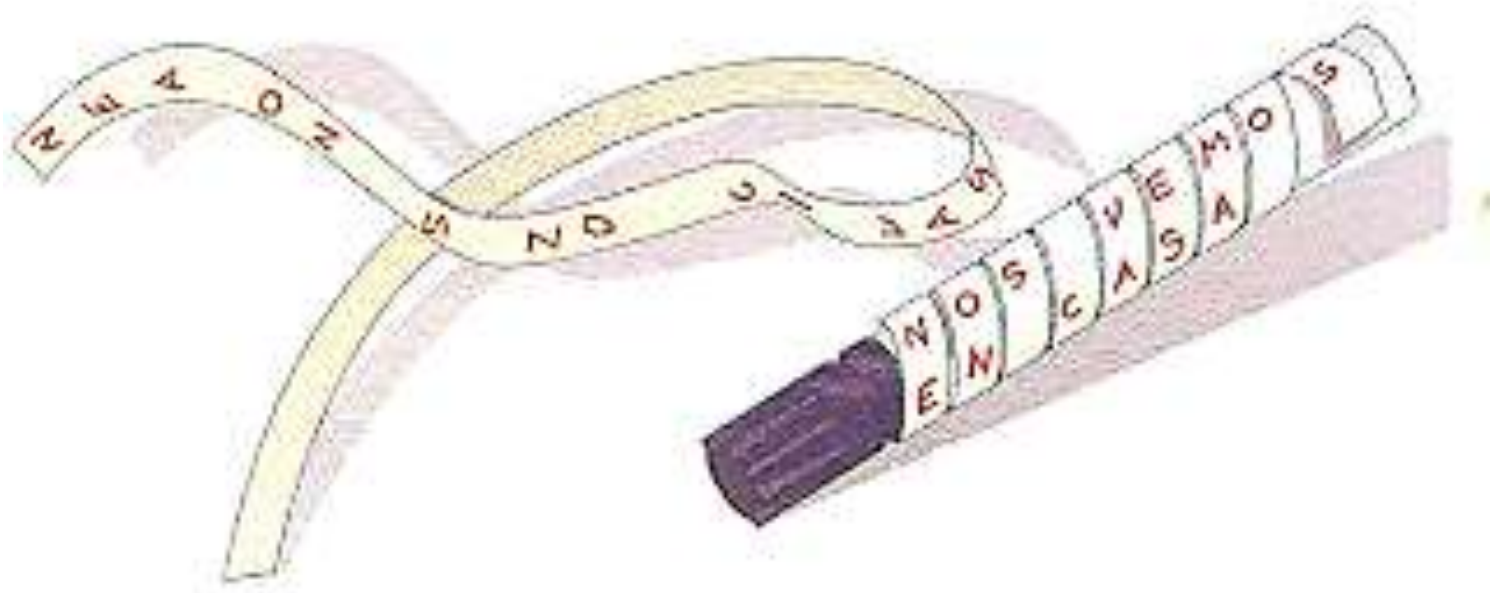
Actividad 01. Cifrados básicos

Escítala

Este método ya lo utilizaban en la antigüedad los griegos, en particular lo empleaban los espartanos para transmitir sus informaciones secretas.

el método consistía, a rasgos generales, en **cortar dos trozos de madera redondos y de similar diámetro**. Para transcribir el mensaje, **usaban una tira de papel y la enrollaban alrededor del trozo de madera, transcribiendo lo que querían comunicar, posteriormente lo desenrollaban y enviaban dicha tira de papel**, de tal manera que **tanto emisor como receptor tenían en su posesión el trozo de madera de similares dimensiones, para poder realizar el cifrado y descifrado de mensajes**.



Cifrado de Polibio

Este cifrado fue creado por el **historiador griego Polibio** en el siglo II antes de Cristo. Polibio ideó este sistema para poder transmitir mensajes ocultos a larga distancia mediante señales ópticas y acústicas. Por ello, el emisor y receptor tendrán que haber acordado una clave que en este caso será una matriz 6×6. Se trata de un cifrado trivial donde **cada carácter se corresponde a una fila y columna de la matriz**.

Ejemplo:

TABLERO DE POLIBIO

	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:

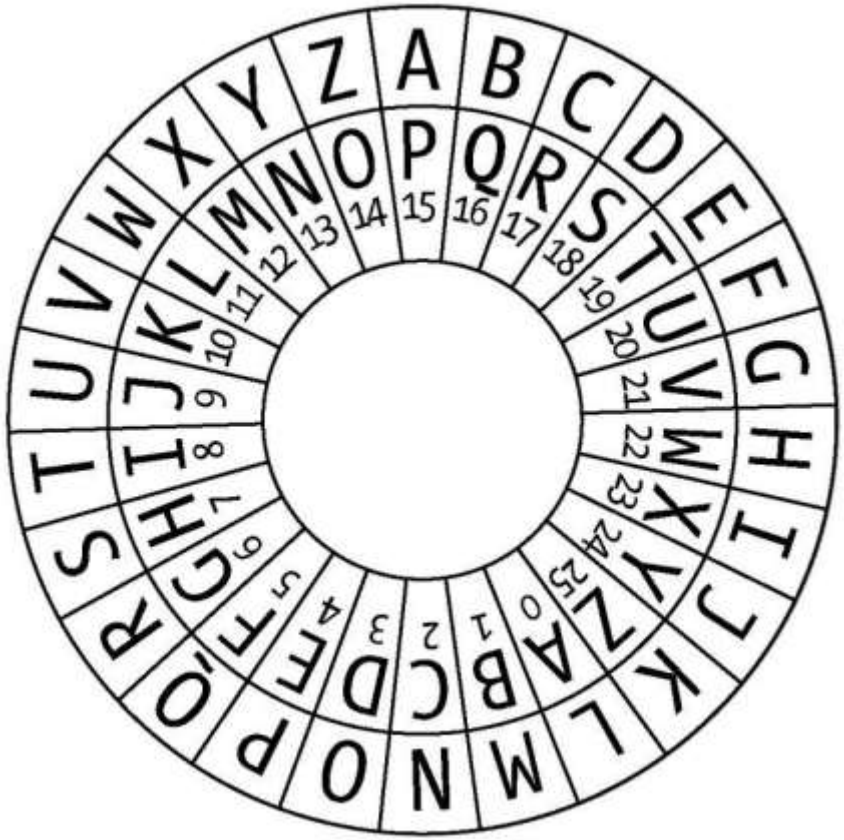
Mañana

Criptograma:

311133113211

Cifrado de César

En criptografía, el **cifrado César**, también conocido como **cifrado por desplazamiento**, código de César o desplazamiento de César, es una de las técnicas de cifrado más simples y más usadas. Es un tipo de **cifrado por sustitución** en el que **una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto**. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etc. Este método debe su nombre a Julio César, que lo usaba para comunicarse con sus generales.

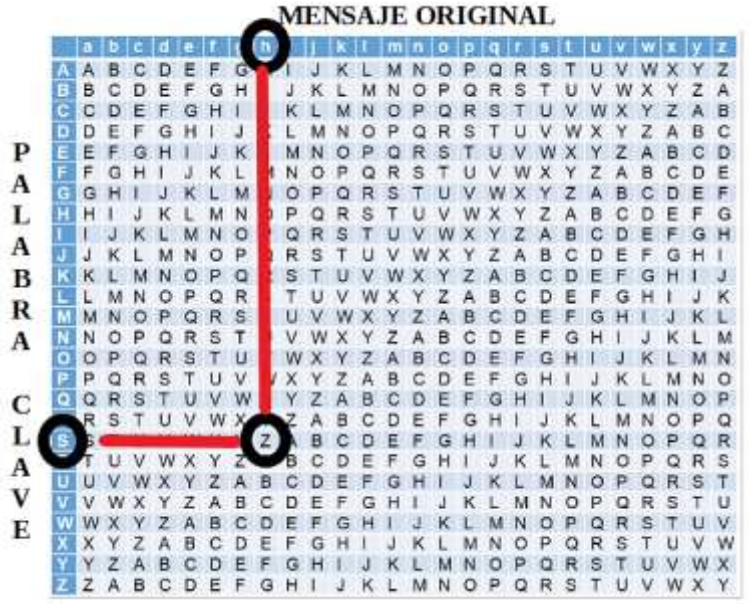


Cifrado de Vigénere

El cifrado de **Vigenère** es un cifrado **basado en diferentes series de caracteres o letras del cifrado César formando estos caracteres una tabla**, llamada **tabla de Vigenère**, que se usa como clave. El cifrado de Vigenère es un **cifrado por sustitución simple polialfabético.**

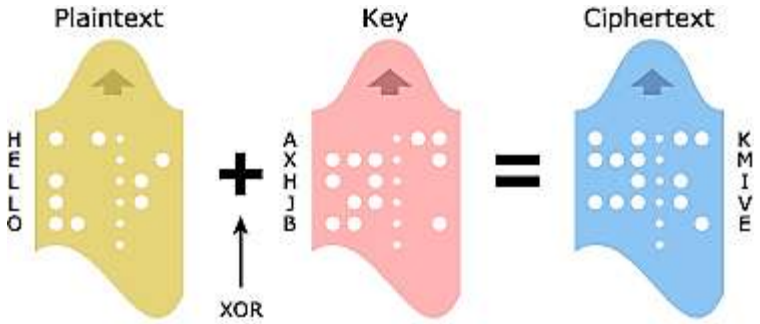
El cifrado de Vigenère se ha reinventado muchas veces. El método original fue descrito por Giovan Battista Belasso en su libro de 1553 La cifra del Sig. Giovan Battista Belasso. Sin embargo, fue incorrectamente atribuido más tarde a Blaise de Vigenère, concretamente en el siglo XIX, y por ello aún se le conoce como el "cifrado de Vigenère".

Este cifrado es conocido porque es fácil de entender e implementar, además parece irresoluble; esto le hizo valedor del apodo el código indescifrable (le chiffre indéchiffrable, en francés).



Cifrado de Vernam

En terminología moderna, un **cifrado de Vernam es un cifrado de flujo** en el que **el texto en claro se combina, mediante la operación XOR, con un flujo de datos aleatorio o pseudoaleatorio del mismo tamaño**, para generar un texto cifrado. El uso de datos pseudoaleatorios generados por un generador de números pseudoaleatorios criptográficamente seguro es una manera común y efectiva de construir un cifrado en flujo. El **RC4** es un ejemplo de cifrado de Vernam que se utiliza con frecuencia en Internet.



Es un método para cifrar texto alfabético. Es una de las técnicas de sustitución para convertir un texto sin formato en un texto cifrado. En este mecanismo asignamos un número a cada carácter del Texto Plano, como (a = 0, b = 1, c = 2, … z = 25).

Método para tomar la clave:

En el algoritmo de cifrado de Vernam, tomamos una clave para cifrar el texto sin formato, cuya longitud debe ser igual a la longitud del texto sin formato.

Algoritmo de cifrado:

1. Asigne un número a cada carácter del texto sin formato y la clave de acuerdo con el orden alfabético.

2. Agregue ambos números (el número de carácter de texto sin formato correspondiente y el número de carácter clave).
3. Resta el número de 26 si el número sumado es mayor que 26, si no lo es, déjalo.

Ejemplo:

```
Plain-Text: RAMSWARUPK
Key: RANCHOBABA
```

Ahora, de acuerdo con nuestro algoritmo de cifrado, asignamos un número a cada carácter de nuestro texto sin formato y clave.

```
PT:   R  A  M   S   W   A  R   U   P   K
NO:   17 0  12  18  22  0  17  20  15  10

KEY:  R   A  N   C  H  O   B  A  B  A
NO:   17  0  13  2  7  14  1  0  1  0
```

Ahora agregue el número de texto sin formato y clave y después de realizar la operación de suma y resta (si es necesario), obtendremos el número de carácter de texto cifrado correspondiente.

```
CT-NO: 34  0  25  20  29  14  18  20  16  10
```

En este caso, hay dos números que son mayores que 26, por lo que debemos restarles 26 y, después de aplicar la operación de resta, los nuevos números de caracteres de texto cifrado son los siguientes:

```
CT-NO:  8  0  25  20  3  14  18  20  16  10
```

El nuevo texto cifrado es después de obtener el carácter correspondiente del número.

```
CIPHER-TEXT: I  A  Z  U  D  O  S  U  Q  K
```

Nota:

Para el descifrado, aplique el proceso inverso al de cifrado.

En los siguientes artículos se habla de los sistemas de cifrado y su evolución:

- Breve historia de la criptografía
- Historia de la criptografía
- Una breve historia de la criptografía
- Criptografía desde su origen hasta la actualidad
- Historia de la criptografía

En los siguientes vídeos se habla de los sistemas de cifrado y su evolución:

- Una Corta Historia del Cifrado de Datos
- Cómo funciona la criptografía
- Así funcionaba ENIGMA y el Sistema de Comunicaciones Nazi
- ¿Cómo funcionaba la Máquina Enigma?

Se pide:

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.

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.

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 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

6. Descifra el siguiente texto:

ZMDTHAH SAEUAAMGO ÑWTYI MLBA

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

5. Cifrado de Vernam

Aplica cifrado Vernam y muestra el texto cifrado:

Palabra	hola	h	o	l	a
	Código ASCII				
	Binario				

CLAVE	948/	9	4	8	/
	Código ASCII				
	Binario				

Palabra					
CLAVE					
XOR					

CIFRADO					