
CÓDIGOS Y SECRETOS
KHOOR ZRUOG
Un paseo por la criptografía clásica
MARCOS TORRENT

CÓDIGOS Y SECRETOS

MARCOS TORRENT

Definición del concepto de 'criptografía' junto con la explicación de una decena de métodos y técnicas precursoras de esta ciencia. **Un viaje al pasado que te enseñará a escribir mensajes en clave de la misma forma que lo hacían espartanos, historiadores griegos, líderes romanos y hermandades.** Bienvenidos a CÓDIGOS y SECRETOS.

1ª EDICIÓN, Diciembre 2022.

2ª EDICIÓN, Febrero 2026.

TecnologiAR

(https://www.tecnologiar.com/)

Índice

La criptografía

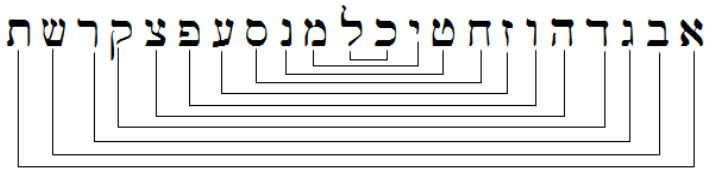
La palabra **criptografía** proviene del griego "*kryptos*" que significa oculto y "*graphia*" que significa escritura. Su definición según el diccionario es: "El arte de escribir con clave secreta o de un modo enigmático". La criptografía es una técnica, o más bien un conjunto de técnicas, que originalmente tratan sobre la protección de la información frente a observadores no autorizados. Por tanto, el único objetivo de la criptografía es conseguir la confidencialidad de los mensajes.

Los primeros métodos criptográficos

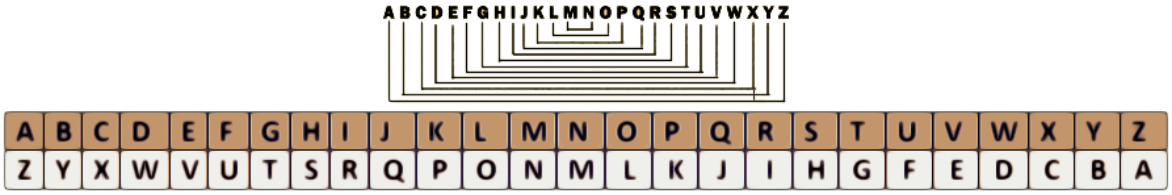
» Cifrado Atbash

'**Atbash'** es un método de cifrado del alfabeto hebreo que se piensa fue utilizado ya a partir del 600 / 500 a.C. Pertenece a la llamada criptografía clásica y es un tipo de ***cifrado por sustitución*** donde el símbolo original es remplazado por otro a modo de clave. Se le denomina también "método de espejo", pues consiste en sustituir la primera letra (álef) por la última (tav), la segunda ([ב|bet]) por la penúltima (shin) y así sucesivamente.

Versión original:



Adaptación:



Para encriptar un mensaje en Atbash debemos remplazar nuestras letras originales por sus equivalentes a modo de clave.

Supongamos que quiero encriptar la palabra ***'LÁMPARA'***. En base a la figura anterior:

L = O | **A** = Z | **M** = N | **P** = K | **A** = Z | **R** = I | **A** = Z

Texto original: LAMPARA | **Texto encriptado:** OZNKZIZ

A la hora de desencriptar, utilizaríamos el mismo método pero de manera inversa.

O = L | **Z** = A | **N** = M | **K** = P | **Z** = A | **I** = R | **Z** = A

Texto encriptado: OZNKZIZ | **Texto original:** LAMPARA

» La escitala

Los espartanos utilizaron, hacia el 400 a.C., la **'escitala'**. Ésta puede considerarse el primer ***sistema de criptografía por transposición***. Es decir, que se caracteriza por ocultar el significado real de un texto alterando el orden de los signos que lo conforman.

Los militares de la ciudad-estado griega escribían sus mensajes sobre una tela que envolvía una vara. El mensaje sólo podía leerse cuando se enrollaba la tela sobre un bastón del mismo grosor (que poseían tanto el emisor como el destinatario lícito del mensaje).

Demostración: https://www.youtube.com/watch?v=RwCBAnxg2DI

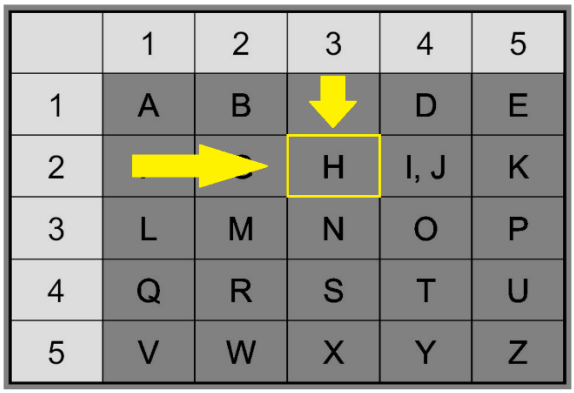
» Cifrado de Polybios

Alrededor del año 150 a. C. se encuentra, tal vez, el ***algoritmo de sustitución*** más antiguo del cual se tiene conocimiento: El **'cifrado de Polybios'**. Éste nombre se dio en reconocimiento al historiador griego del mismo nombre y quien se considera fue su creador.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I, J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Comentario: Si el cifrado Atbash, mencionado anteriormente, data realmente de 600 / 500 a.C, el cifrado de Polybios sería, entonces, el segundo más antiguo basado en la sustitución de símbolos.

Podemos apreciar que en nuestra matriz 5x5 a cada una de nuestras celdas le corresponde una única intersección fila-columna. Por ejemplo, la intersección 1 – 1, fila 1 – columna 1, hace referencia a la letra 'A'. La intersección 2 - 3 hace referencia a la letra 'H'.



Ahora, supongamos que quiero encriptar el siguiente texto: ***'CRIPTOGRAFÍA CLÁSICA'.*** Todo lo que tenemos que hacer es reemplazar las letras de nuestro mensaje por sus correspondientes intersecciones fila-columna.

C	**R**	**I**	**P**	**T**	**O**	**G**	**R**	**A**	**F**	**I**	**A**
13	42	24	35	44	34	22	42	11	21	24	11

C	**L**	**A**	**S**	**I**	**C**	**A**
13	31	11	43	24	13	11

Texto encriptado:

1342243544342242112124111 13311143241311

En caso de tener que "desencriptar", aplicaríamos el método anteriormente visto pero, esta vez, de manera inversa.

Texto encriptado:

1342243544342242112124111 13311143241311

Me ayudo separando el texto en grupos de dos en dos:

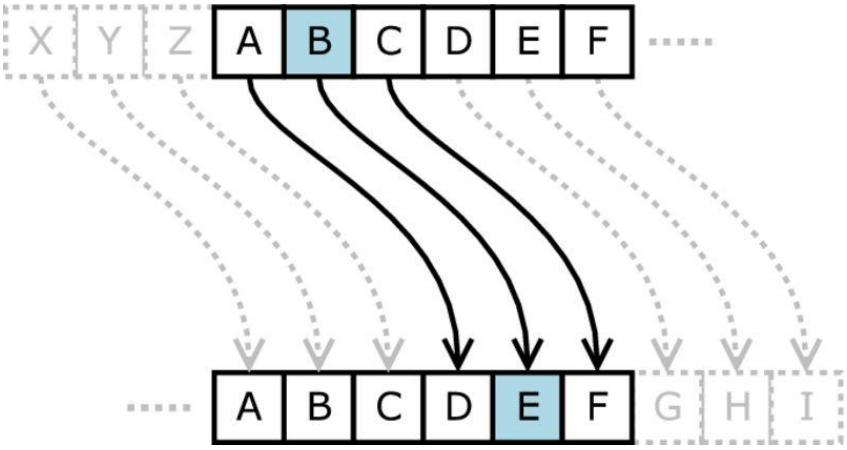
13 42 24 35 44 34 22 42 11 21 24 11 13 31 11 43 24 13 11

Texto original (ayudándome con la tabla):

'Criptografía clásica'

» Cifrado César

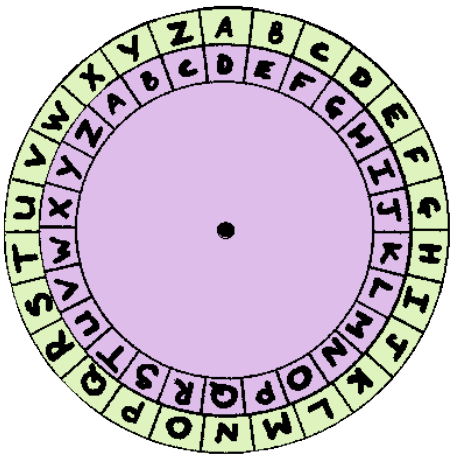
En criptografía, el '**Cifrado César'**, también conocido como 'cifrado por desplazamiento', 'código de César' o 'desplazamiento de César', es una de las técnicas de cifrado más simples y más usadas. Es un tipo de ***cifrado por sustitución*** en el que una letra en el texto original es reemplazada por 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.



En pocas palabras, a la hora de encriptar el texto, cada letra del mensaje original se corresponderá con la letra que, alfabéticamente, esté 3 posiciones más adelante que ella. Por eso decimos que A = D, B = E, C = F y demás.

El cifrado César recibe su nombre en honor al emperador romano 'Julio César' que, según se dice, utilizó este cifrado para proteger mensajes con importante contenido militar. En aquella época, siglo I a. C, este cifrado debió ser razonablemente seguro ya que pocos enemigos de César habrían sabido leer y mucho menos podrían haber llevado a cabo el criptoanálisis necesario para descifrar el código.

Para comprender un poco más este cifrado, nos ayudaremos de la siguiente figura:



La rueda externa representa todas las posibles letras que puede contener nuestro mensaje, así como la rueda interna representa las tradicionales y correspondientes equivalencias a la hora de "encriptar". Entonces, por ejemplo, dada la figura, todas las letras 'A' de nuestro mensaje tendrían que ser escritas como una 'D' al momento de la encriptación.

Hagamos una prueba.

Supongamos que quiero encriptar el siguiente mensaje: ***'CIFRADO CESAR'.*** Todo lo que tenemos que hacer es reemplazar cada letra por su letra clave (guiándonos con la figura).

C	**I**	**F**	**R**	**A**	**D**	**O**
F	L	I	U	D	G	R

C	**E**	**S**	**A**	**R**
F	H	V	D	U

Texto encriptado:

FLIUDGR FHVDU

¿Y para desencriptar?

Lo mismo pero de manera inversa. Tomamos el mensaje encriptado y vamos buscando en nuestra guía de equivalencias todas las letras originales correspondientes. Así, una por una, terminaremos dando con el mensaje puro.

Comentario: El cifrado César mostrado en estas figuras representa el típico desplazamiento tradicional de 3 posiciones a la derecha, A = D. Esto no siempre es así dado que la cantidad de desplazamientos, al igual que la dirección de los mismos, dependerá de un mutuo acuerdo entre el emisor y el receptor.

» Cifrado de Alberti

El **'cifrado de Alberti'** es un método de cifrado descrito por el italiano 'Leon Battista Alberti', arquitecto, humanista, tratadista y matemático, en su tratado *De Cifris* en 1466. Constituye el primer ***cifrado por sustitución polialfabética*** conocido.

La expresión "sustitución polialfabética" hace referencia a que, al momento de encriptar, las letras del texto original no siempre derivarán en la misma letra clave. Suponiendo, en un texto encriptado 'QWETFFAD' tanto la '**Q**' como, por ejemplo, la '**D**' podrían estar **ambas** haciendo referencia a letras 'A' del texto original.

"Hago dos discos con dos láminas de cobre. Uno, el mayor, será fijo y el otro móvil. El diámetro del disco fijo será superior en un noveno al disco móvil. Divido la circunferencia de los discos en 24 partes iguales llamadas sectores. En cada uno de los sectores del ***disco grande*** *escribo en orden alfabético normal una letra mayúscula roja: primero la A, seguida de la B, después la C, etc., omitiendo H, K e Y que no son indispensables"*

Como en latín no existen las letras J, U, W, él rellena por este método solamente 20 sectores. En los otros cuatro escribe los números 1, 2, 3, 4.
Alberti prosigue con su relato de como rellenar el **disco pequeño**.

"... una letra minúscula, pero no en su orden normal como en el disco fijo, sino en un orden incoherente. De esta forma se puede suponerse que la primera letra será la a, la segunda la g, tercera la q y así hasta rellenar los 24 sectores, porque el alfabeto latino consta de 24 caracteres, siendo el vigesimocuarto 'et' ('&'). Efectuadas estas operaciones, se coloca el disco pequeño sobre el grande de modo que una aguja pasada por los dos centros sirva como eje común alrededor del cual girará el disco móvil."

Alfabeto latino

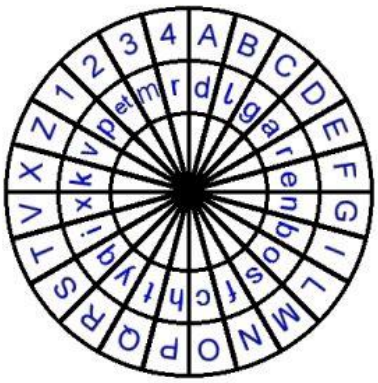
A	B	C	D	E	F	G	H	I	K	L	M
ā	bē	cē	dē	ē	ef	gē	hā	ī	kā	el	em
[a:]	[be:]	[ke:]	[de:]	[e:]	[ɛf]	[ge:]	[ha:]	[i:]	[ka:]	[ɛl]	[ɛm]
N	O	P	Q	R	S	T	V	X	Y	Z	
en	ō	pē	qū	er	es	tē	ū	ex	ī Graeca	zēta	
[ɛn]	[o:]	[pe:]	[kʷu:]	[ɛr]	[ɛs]	[te:]	[u:]	[ɛks]	[i: ˈgrajka]	[ˈze:ta]	

+ et ('&'). = 24 caracteres.

Ahora, él escoge en el disco pequeño una letra clave. Por ejemplo, la **'k'**. Esta letra la alinea con cualquiera de las letras exteriores, por ejemplo con la **'B'**, e informa de esta alineación al receptor del mensaje mediante una 'B' mayúscula al principio del texto encriptado.

... Usando este punto de partida, cada letra del mensaje representará a la minúscula que hay sobre ella. Después de escribir tres o cuatro letras, puedo cambiar la posición de la letra clave de modo que la ***k*** *esté, por ejemplo, sobre la D. Después en mi mensaje escribo una D mayúscula y, a partir de este punto,* ***k*** *ya no significará B y si D, y todas la letras del disco fijo tienen nuevas identidades.*

Explicaremos todo esto mediante un ejemplo. Por ahora, sólo acuérdense que el disco grande corresponde a las letras originales y que el disco pequeño hace referencia a las letras de "encriptación".



Texto real: 'LEONBATTISTAALBERTI' | **Texto encriptado:** **X**orcf**A**vkfflsfk**N**oishmdq

■ **Analicemos cómo fue la encriptación**:

1) En la rueda pequeña y movediza tomamos como letra clave a la letra **'k'** *(la letra utilizada como clave es de conocimiento mutuo entre emisor-receptor y no se cambiará en todo el proceso de encriptado/desencriptado)* y, mediante una 'X' mayúscula al inicio del texto encriptado, indicaremos que la **'k'** está alineada con la **'X'** de la rueda grande y fija. Por ende, hasta que no aparezca otra mayúscula en el texto, el receptor sabrá que la encriptación estuvo alineada de esa manera.
Encriptamos las primeras 4 letras:

L = O | E = R | O = C | N = F → Xorcf

2) Cambiamos la alineación de los discos. Ahora nuestra clave **'k'** estará alineada con la **'A'** del disco mayor. Indicamos esto mediante una letra 'A' mayúscula en el texto y encriptamos 8 letras más:

B = V | A = K | T = F | T = F | I = L | S = S | T = F | A = K → XorcfAvkfflsfk

3) Alineamos la 'k' con la **'N'** y encriptamos las 7 últimas letras:

A = O | L = I | B = S | E = H | R = M | T = D | I = Q → XorcfAvkfflsfkNoishmdq

'XorcfAvkfflsfkNoishmdq'

■ **Desencriptado:** Mismo proceso pero de manera inversa. Alineamos los discos según encontramos mayúsculas en nuestro mensaje, buscamos nuestra letra encriptada en la rueda chica y descubrimos la verdadera letra en nuestra rueda grande y fija.

Para poder desencriptar el mensaje el receptor necesita un disco exactamente igual al que sirvió para crear el cifrado. No vale cualquier disco con una distribución arbitraria de las letras. Otro problema, es que si alguien posee un disco igual al que creó el criptograma, lo descifraría con facilidad. La seguridad de este cifrado depende de mantener secretos los discos. En la actualidad esto se considera una falta grave de cualquier método de cifrado.

» Cifrado de Vigenère

LETRAS TEXTO PURO

LETRAS CLAVE

	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

'El cifrado de Vigènere' es un método que utiliza una serie de diferentes ***Cifrados César*** en base a las letras de una palabra clave. El método fue descrito por primera vez en 1533 por 'Giovan Battista Bellaso', criptólogo italiano, aunque, por alguna razón, se le atribuye su invención a 'Blaise de Vigenère' (1523–1596), diplomático, criptógrafo y químico francés. El cifrado es relativamente simple de entender e implementar y, por tres siglos, se lo consideró uno de los mejores dada su resistencia a ser descifrado.

Para encriptar un mensaje en cifrado Vigènere necesitamos dos cosas:

1) El propio mensaje a encriptar.
2) Una palabra clave.

Supongamos que quiero encriptar el siguiente mensaje: ***'ESTOY TOMANDO MATE'***. Escogeré como clave la palabra ***'PAVA'***. Ahora:

1) Colocamos nuestra palabra clave repetidamente a lo largo de todo el mensaje:

E	S	T	O	Y	T	O	M	A	N	D	O	M	A	T	E
P	A	V	A	P	A	V	A	P	A	V	A	P	A	V	A

2) Buscamos en nuestra tabla/guía de Vigènere la intersección correspondiente entre la letra del mensaje original y la letra de la palabra clave. Para el primer caso sería 'E' (original) y 'P' (clave) que dan como resultado la letra 'T'. Ahí tenemos nuestra primera letra.

E	S	T	O	Y	T	O	M	A	N	D	O	M	A	T	E
P	A	V	A	P	A	V	A	P	A	V	A	P	A	V	A

LETRAS TEXTO PURO

LETRAS CLAVE

	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

Texto encriptado final:

'Tsoon tjmpnyo baoe'

Para desencriptar:

Como siempre, mismo método aplicado de manera inversa.

Mensaje encriptado: Tsoon tjmpnyo baoe

Clave: Pava

T	S	O	O	N	T	J	M	P	N	Y	O	B	A	O	E
P	A	V	A	P	A	V	A	P	A	V	A	P	A	V	A

LETRAS TEXTO PURO

LETRAS CLAVE

	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

Texto final original:

'Estoy tomando mate'

Cifrado y descifrado Vigènere: https://www.youtube.com/watch?v=fJB6Z7HctDU

» Código Bacon

El **'Código Bacon'** o **'clave Baconiana'** (en inglés **'Baconian cipher'**), es un método criptográfico desarrollado por 'Francis Bacon' (1561-1626), filósofo, político, abogado y escritor inglés.

De acuerdo a Sir Francis Bacon, existen tres propiedades que debe de tener un cifrado:

1***) Debe de ser fácil de escribir y de leer***

2) Debe de ser confiable y que no pueda ser descifrado.

3) Si es posible debe ser libre de sospecha debido a que si un mensaje llegara a caer en manos incorrectas, éste no pueda ser descifrado a pesar de ser examinado por expertos.

Para encriptar un mensaje en Bacon cada letra del texto original debe ser reemplazada por un grupo de cinco letras de acuerdo con la siguiente tabla:

a:	AAAAA	h:	AABBB	o:	ABBBA	v:	BABAB
b:	AAAAB	i:	ABAAA	p:	ABBBB	w:	BABBA
c:	AAABA	j:	ABAAB	q:	BAAAA	x:	BABBB
d:	AAABB	k:	ABABA	r:	BAAAB	y:	BBAAA
e:	AABAA	l:	ABABB	s:	BAABA	z:	BBAAB
f:	AABAB	m:	ABBAA	t:	BAABB		
g:	AABBA	n:	ABBAB	u:	BABAA		

Supongamos, por ejemplo, que queremos encriptar el siguiente mensaje: '***Te espero a las cinco***'

1) Al codificarlo utilizando Bacon:

BAABA AABAA AABAA BAAAB ABBBA AABAA BAAAA ABBAB AAAAA ABABA AAAAA BAAAB AAABA ABAAA ABBAA AAABA ABBAB

Si se eliminan los espacios:

BAABAAABAAAABAABAAABABBBAAABAABAAAAABBABAAAAAABABAAAAAABAAABAAABAA BAAAABBAAAAABAABBAB

2) Luego, debemos construir un mensaje falso que tenga el mismo número de letras que el mensaje encriptado. Por ejemplo:

NODESEOVERTEMASMEHASDECEPCIONADOPREFIEROESTARSOLOADIOSSSSSSSSSSSSSSSSS SSSSSSSSSSSSS

Ahora, ¿para qué nos servirá este mensaje falso?

Mediante el uso de mayúsculas y minúsculas, indicaremos que letra correspondería a una 'A' y que letra correspondería a una 'B' en nuestro código Bacon. Así, el mensaje falso, además de

convertir a nuestro código en un mensaje libre de sospecha, podrá ser traducido a Bacon para luego obtener el mensaje final.

Ejemplo (B's = Mayúsculas | A's = Minúsculas):

NodEseoVerteMasMehaSdECEpciOnaDoprefIErOestarsOlOadiossSsssSsssSssSsssssSSssssssSssSSsS

Colocando los espacios:

No dEseo Verte Mas Me haS dECEpciOnaDo prefIErO estar sOlO adiossSsssSsssSssSsssssSSssssssSssSSsS

Genial. Terminamos el proceso de encriptado en Bacon. Ahora veamos qué es lo que debe hacer la persona que recibirá nuestro mensaje. Acuérdense que los procesos de desencriptado son, por lo general, la forma inversa del método de encriptación.

1) Texto recibido:

No dEseo Verte Mas Me haS dECEpciOnaDo prefIErO estar sOlO adiossSsssSsssSssSsssssSSssssssSssSSsS

2) Texto sin espacios:

NodEseoVerteMasMehaSdECEpciOnaDoprefIErOestarsOlOadiossSsssSsssSssSsssssSSssssssSssSSsS

3) Traslado a Bacon (B's = Mayúsculas | A's = Minúsculas):

BAABAAABAAAABAABAAABABBBAAABAABAAAAABBABAAAAAABABAAAAAABAAABAAABAABAAAABBAAAAABAABBAB

4) Ordenamiento en grupos de 5 en 5 (formato de los grupos Bacon):

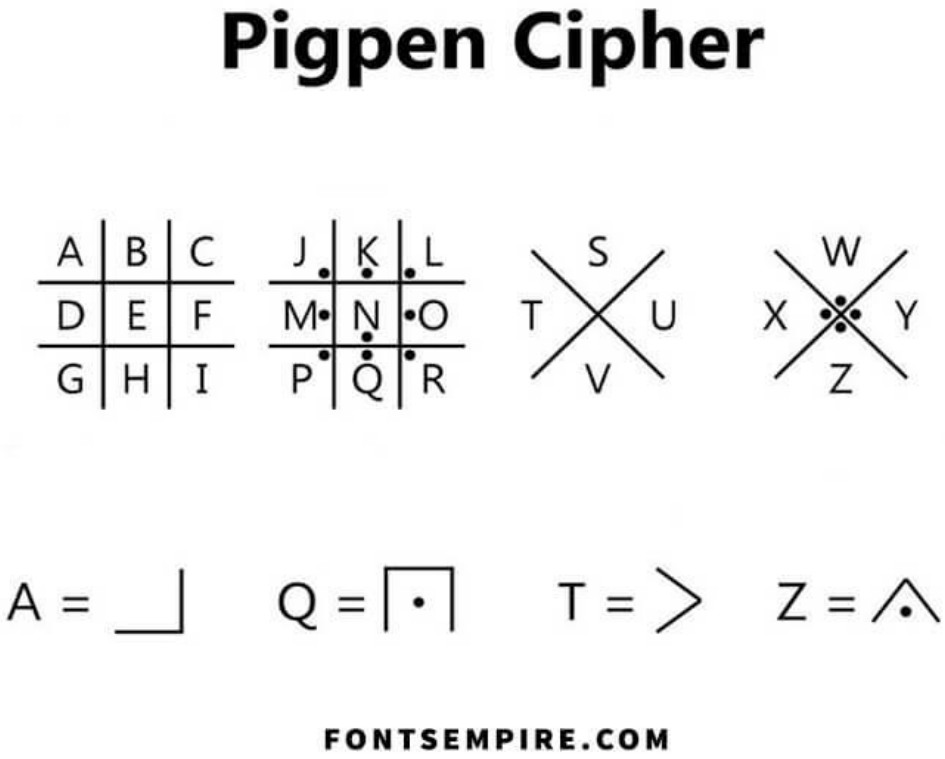
BAABA AABAA AABAA BAAAB ABBBA AABAA BAAAA ABBAB AAAAA ABABA AAAAA BAAAB AAABA ABAAA ABBAA AAABA ABBAB

a:	AAAAA	h:	AABBB	o:	ABBBA	v:	BABAB
b:	AAAAB	i:	ABAAA	p:	ABBBB	w:	BABBA
c:	AAABA	j:	ABAAB	q:	BAAAA	x:	BABBB
d:	AAABB	k:	ABABA	r:	BAAAB	y:	BBAAA
e:	AABAA	l:	ABABB	s:	BAABA	z:	BBAAB
f:	AABAB	m:	ABBAA	t:	BAABB		
g:	AABBA	n:	ABBAB	u:	BABAA		

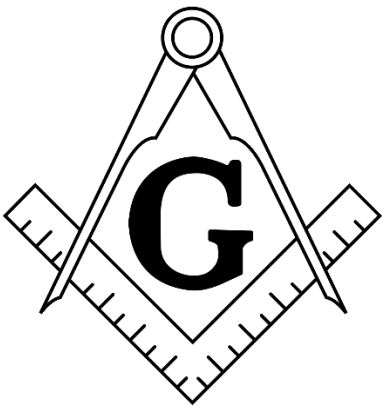
Texto final: ***'Te espero a las cinco'***

» Cifrado Francmasón

El **'Cifrado Francmasón'** (también denominado **'Cifrado masónico'**, **'Cifrado Pigpen'**, **'Cifrado de Napoleón'** y **'Cifrado tic-tac-toe'**) ***es un cifrado geométrico de sustitución simple*** que intercambia letras por símbolos que son fragmentos de una cuadrícula.



Este cifrado fue desarrollado por francmasones a principios del siglo XVIII para mantener en privado sus registros de historia, ritos y correspondencia entre los líderes de la logia.



¿Qué es la masonería?

https://www.masoneria-argentina.org.ar/que-es-la-masoneria

Respecto a los procesos de "encriptado" y "desencriptado", éstos son realmente simples. Teniendo presente la guía de simbolos, sólo debemos reemplazar por sus correspondientes equivalencias y así encriptaremos/desencriptaremos nuestro mensaje.

» Cifrado Playfair

El **cifrado Playfair** fue inventado en 1854 por 'Charles Wheatstone', científico e inventor británico, para encriptar mensajes enviados por telegrama. Sin embargo, este código lleva el nombre de su amigo 'Lord Playfair' quien promovió dicho cifrado para uso militar.

■ **Creación de la matriz de cifrado**

MENSAJE A ENCRIPTAR: **'CORREDIZO'**

1) Como primer medida, debemos crear una tabla /matriz de 5x5.

2) Escogeremos una palabra clave, sin importar su cantidad de letras, la cual ocupará los primeros espacios de la matriz. Por ejemplo: '***CIFRADO***'.

C	I	F	R	A
D	O			

En caso de que nuestra palabra clave contenga letras repetidas (ej: C**A**S**A**), quitaremos dichas repeticiones y utilizaremos como clave el sobrante de esa palabra. (CASA = **CAS**)

3) Ya situada nuestra clave en la matriz, rellenaremos el resto de la grilla con todas las letras restantes del alfabeto que no sean parte de nuestra clave.

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

» Las letras, a excepción de las que forman parte de la clave, deben respetar su correspondiente orden alfabético.
» No puede haber letras repetidas en la tabla.
» La 'J' es colocada con la 'I' al igual que en el cifrado de Polybios. Esto se hace para poder preservar la cantidad de 25 espacios (5x5)

4) Tomamos el mensaje que queremos encriptar ('CORREDIZO') y lo dividimos en bloques de dos letras cada uno.

CO RR ED IZ O (Acá tenemos dos **problemas**)

» No puede haber dos letras iguales en el mismo bloque. Entonces, debemos colocar una 'X' (o una letra poco usual) entre ambas y volver a realizar la división de grupos.

» No puede quedarnos un número impar de letras. Tenemos que tener, sí o sí, todos bloques dos unidades. En este caso, si no fuera porque la resolución al primer problema también resolvió el segundo, deberíamos colocar una X (o una letra poco usual) en el último grupo que quedó sin letra (O -> OX).

Mensaje corregido:

CO R**X** RE DI ZO

5) Teniendo el mensaje listo para encriptar, empezaremos a trabajar con cada bloque particular haciendo uso de las siguientes reglas:

A) Si las dos letras del bloque aparecen en la misma fila de la tabla, **cada una se reemplaza por la letra adyacente que se encuentra a su derecha** (si es la letra

que se encuentra en la última posición a la derecha de la fila se la reemplaza con la primera de la izquierda de esa fila).

Ejemplo:

Supongamos que tenemos un bloque "**KN**"

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

KN -> **LH**

B) Si las dos letras del bloque aparecen en la misma columna de la tabla, **cada una se reemplaza por la letra adyacente que se encuentra por debajo** (si es la letra que se encuentra en la última posición inferior de la columna se la reemplaza con la primera de arriba de esa columna).

Ejemplo:

Supongamos que tenemos un bloque "**RM**"

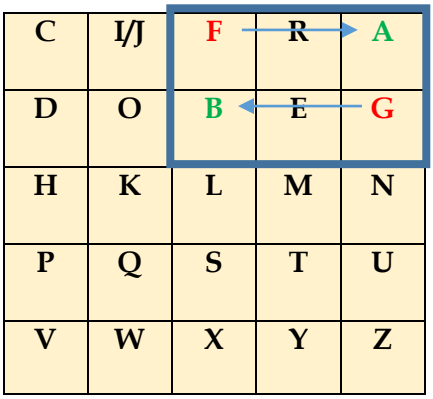
C	I/J	F	R ↓	A
D	O	B	E	G
H	K	L	M ↓	N
P	Q	S	T	U
V	W	X	Y	Z

RM -> **ET**

C) Si las letras no se encuentran en la misma fila ni columna, se determina el rectángulo formado por ambos caracteres y se los encripta tomando los caracteres que están en sus respectivas esquinas opuestas.

Ejemplo:

Supongamos que tenemos un bloque "**FG**"



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

FG -> **AB**

Encriptación de nuestro mensaje: CO RX RE DI ZO

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

CO = ID o JD (cualquiera es válido) | RX = FY | RE = EM | DI = OC | ZO = WG

Texto encriptado:

ID FY EM OC WG

Sin espacios:

IDFYEMOCWG

■ **Descifrado / Desencriptado** ('IDFYEMOCWG'):

Para poder desencriptar el mensaje recibido necesitaremos:

» El propio mensaje a descifrar / desencriptar en sí.

» La clave principal que ocupa los primeros espacios de la grilla

» Conocer el método empleado para la encriptación de manera que podamos emplearlo de **forma inversa**.

A) Si las dos letras del bloque aparecen en la misma fila de la tabla, **cada una se reemplaza por la letra adyacente que se encuentra a su izquierda.**

B) Si las dos letras del bloque aparecen en la misma columna de la tabla, **cada una se reemplaza por la letra adyacente que se encuentra por arriba.**

C) Si las letras no se encuentran en la misma fila ni columna, se determina el rectángulo formado por ambos caracteres y se los encripta tomando los caracteres que están en sus respectivas esquinas opuestas.

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

Mensaje encriptado:

IDFYEMOCWG

Separo en grupos:

ID FY EM OC WG

Proceso de desencriptado:

ID = CO | FY = RX | EM = RE | OC = DI / DJ | WG = ZO

Dos posibles soluciones:

CORXRE**DI**ZO | CORXRE**DJ**ZO

Quito símbolos poco usuales ('X') utilizados para separar letras repetidas

COR**X**REDIZO | COR**X**REDJZO

CORREDIZO | CORREDJZO

Mensaje original:

CORREDIZO

Comentario: Además de situarse juntas la 'I' con la 'J' por cuestiones de espacio, no es casualidad que justo se haya escogido este par. La razón es que al momento de desencriptar un texto se notaría claramente un error en el mensaje final si hubiésemos puesto una I cuando en realidad iba una J o viceversa. Esto está pensado, sobre todo, para el idioma inglés.

» Cifrado ADFGVX

La **'cifra ADFGVX'**, inventada en 1917 por el teniente 'Fritz Nebel' (1891–1977), fue escogida por el Alto Mando alemán como la más segura para cifrar sus comunicaciones antes de las grandes ofensivas de 1918 durante la Primera Guerra Mundial.

La seguridad de la cifra, relativamente grande para tratarse de una cifra que puede operarse con papel y lápiz, se debe a su naturaleza enrevesada, con una mezcla de ***sustitución*** (los símbolos originales son reemplazados por otros) y ***transposición*** (se altera el orden de los símbolos).

No obstante su seguridad, la cifra fue descifrada a tiempo por el criptógrafo francés 'Georges Painvin', miembro del 'Deuxieme Bureau' (servicio de información del Ejército francés), para influir en el desarrollo de los acontecimientos. En concreto, fue un mensaje relativo a la remisión de municiones lo que permitió a los franceses averiguar el lugar de la ofensiva realizada por las tropas alemanas entre el 9 y el 13 de junio de 1918.

Se trata de la, cronológicamente, última cifra importante aparecida antes del desarrollo de las máquinas criptográficas.

	A	D	F	G	V	X
A						
D						
F						
G						
V						
X						

Viendo la grilla, puede que hayas recordado al cifrado Polybios. Además, para nuestra suerte, no están tan alejados uno del otro. Utilizaremos una clave que ocupará los primeros espacios de la grilla, **como hicimos en el cifrado Playfair**, para luego terminar de completar esta última y encriptar nuestra primer parte del mensaje **al estilo Polybios** (una letra = intersección fila – columna). Todas cosas que ya conocemos.

Después, para terminar el encriptado, sumaremos ese "plus" que nos otorga ADFGVX. Estamos hablando de una segunda clave y una segunda tabla que terminarán de cerrar el proceso.

Encriptado:

» MENSAJE A ENCRIPTAR: '**YERBA MATE'**

» CLAVE PARA LA GRILLA: '**VERANO'**

En caso de que nuestra palabra clave contenga letras repetidas (ej. PANADERÍA), quitaremos dichas repeticiones y utilizaremos como clave el sobrante de esa palabra. (PANADERÍA = PANDERI)

La palabra clave, al igual que en el cifrado Playfair, debe ocupar los primeros espacios de nuestra matriz.

	A	D	F	G	V	X
A	V	E	R	A	N	O
D						
F						
G						
V						
X						

Ya situada nuestra **clave** en la matriz, rellenaremos el resto de la grilla con todas las letras restantes del alfabeto (respetando su orden) y que no sean parte de nuestra clave. Posteriormente a esto, los espacios restantes serán rellenados con los dígitos del 0 al 9.

Notese que en Polybios y Playfair, al ser matrices de 5x5 (25 espacios), sólo teníamos lugar para las letras. La matriz 6x6 del ADFGVX nos permite colocar 36 símbolos.

	A	D	F	G	V	X
A	V	E	R	A	N	O
D	B	C	D	F	G	H
F	I	J	K	L	M	P
G	Q	S	T	U	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

¡Encima de poder agregar números, la 'J' y la 'I' tienen celda propia!

Primera encriptación (al estilo Polybios):

'YERBA MATE' = VA AD AF DA AG FV AG GF AD

¡Pausa!

¿Por qué está bueno ponerle clave a una matriz?

Tengamos en cuenta que si sólo existiesen versiones "estándar" de las matrices para cifrar, cualquiera que conozca el tipo de cifrado empleado podría descifrar nuestros textos con suma facilidad. Bastaría con tomar la matriz general y empezar a reemplazar valores.

Mediante el uso de una clave para nuestra matriz, alteramos todo, o gran parte, del orden de sus símbolos obteniendo matrices únicas y personalizadas. Conocer el tipo de cifrado no bastaría para resolver el problema sino que también, para obtener correctamente el mensaje que se ocultó, necesitaríamos conocer la clave. Esto es, en pocas palabras, la distribución final de los símbolos en la matriz.

Sigamos. Ya tenemos la primera parte de la encriptación. Ahora, a razón de proteger aún más el mensaje, pensaremos en una segunda clave. Esta última, al igual que la clave empleada en la grilla, no debe poseer letras repetidas y, en caso de tenerlas, estas repeticiones deberán eliminarse.

SEGUNDA CLAVE: 'MESA'

¿Qué haremos con esta clave?

1) Haremos una grilla con un número de columnas equivalente a la longitud de nuestra clave. En este caso, 4. La clave debe ser título y parte de la grilla.

M	E	S	A

2) Colocaremos nuestro mensaje encriptado en la grilla, letra por letra, de izquierda a derecha. Esto terminará mostrando la cantidad total de filas.

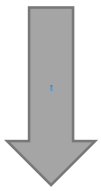
'VA AD AF DA AG FV AG GF AD'

M	E	S	A
V	A	A	D
A	F	D	A
A	G	F	V
A	G	G	F
A	D		

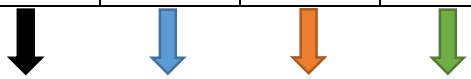
3) Alteraremos la posición de las columnas según el orden alfabético de las letras que forman parte de nuestra clave. MESA = AEMS

A	E	M	S
D	A	V	A
A	F	A	D
V	G	A	F
F	G	A	G
	D	A	

4) Extraeremos el texto de la siguiente manera respetando el orden de las columnas.



A	E	M	S
D	A	V	A
A	F	A	D
V	G	A	F
F	G	A	G
	D	A	



Texto final: 'DAVF AFGGD VAAAA ADFG'

Desencriptado:

Nosotros, al igual que el remitente del mensaje, conocemos las claves de ambas grillas. Esto, como todo cifrado que posee contraseña, ya es de acuerdo mutuo entre el emisor y el receptor. Todo lo que nos resta hacer es emplear el método de encriptación pero, como siempre, de manera inversa.

Mensaje recibido: 'DAVF AFGGD VAAAA ADFG'

1) Como nosotros conocemos el proceso de encriptado, sabemos que el mensaje final fue producto de extraer, columna por columna, la grilla secundaria ('MESA') ordenada alfabéticamente ('AEMS'). Ahora tengo que crear la misma tabla 'AEMS' e introducir la primer tira de letras en la primer columna y así sucesivamente.

A	E	M	S
D	A	V	A
A	F	A	D
V	G	A	F
F	G	A	G
	D	A	

2) Ordenamos las columnas para llegar a nuestra verdadera clave secundaria.

M	E	S	A
V	A	A	D
A	F	D	A
A	G	F	V
A	G	G	F
A	D		

3) Extraemos nuestro mensaje fila por fila de izquierda a derecha.

'VAAD AFDA AGFV AGGF AD'

Sin espacios:

'VAADAFDAAGFVAGGFAD'

4) Agrupamos el texto en bloques de dos unidades cada uno y tomamos nuestra primer grilla la cual ya sabemos cómo está diseñada al ser de acuerdo mutuo.

	A	D	F	G	V	X
A	V	E	R	A	N	O
D	B	C	D	F	G	H
F	I	J	K	L	M	P
G	Q	S	T	U	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

'VA AD AF DA AG FV AG GF AD'

5) ¡Hora de desencriptar!

	A	D	F	G	V	X
A	V	E	R	A	N	O
D	B	C	D	F	G	H
F	I	J	K	L	M	P
G	Q	S	T	U	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

'VA AD AF DA AG FV AG GF AD'

VA = Y | **AD** = E | **AF** = R | **DA** = B | **AG** = A

FV = M | **AG** = A | **GF** = T | **AD** = E

'Y E R B A M A T E'

Mensaje desencriptado:

'YERBA MATE'

Bibliografía

» **Introducción a la criptografía.** http://www.dma.fi.upm.es, http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/criptografia.html.

» **Criptografía. Wikipedia,** https://es.wikipedia.org/wiki/Criptograf%C3%ADa#Historia_de_la_criptograf%C3%ADa

» **Atbash. Wikipedia,** https://es.wikipedia.org/wiki/Atbash

» **(5/10/11). Polybios. U.N.A.M Criptografía,** https://unamcriptografia.wordpress.com/category/tecnicas-clasicas-de-cifrado/sustitucion/monoalfabetica/monogramica/polybios/.

» **Cifrado César. Wikipedia,** https://es.wikipedia.org/wiki/Cifrado_C%C3%A9sar

» **(11/12/17). Manuel López Michelone. Otro esquema de encripción interesante: El cifrado Vigenère. Unocero,** https://www.unocero.com/noticias/otro-esquema-de-encripcion-interesante-el-cifrado-vigenere/

» **Francis Bacon. Wikipedia,** https://es.wikipedia.org/wiki/Francis_Bacon

» **Código Bacon. Wikipedia,** https://es.wikipedia.org/wiki/C%C3%B3digo_Bacon

» **Pigpen Cipher. Wikipedia,** https://en.wikipedia.org/wiki/Pigpen_cipher

» **Cifrado de Playfair. Wikipedia,** https://es.wikipedia.org/wiki/Cifrado_de_Playfair

» **(28/06/05). Criptosistema Playfair. Textos científicos,** https://www.textoscientificos.com/criptografia/playfair

» **ADFGVX. Wikipedia,** https://es.wikipedia.org/wiki/ADFGVX

» **ADFGVX Cipher. Crypto Corner,** https://crypto.interactive-maths.com/adfgvx-cipher.html

» **Cifrado de Alberti. Wikipedia,** https://es.wikipedia.org/wiki/Cifrado_de_Alberti

» **(2015). José Luis Tabara Carbajo. Alberti.** https://joseluistabaracarbajo.gitbooks.io/, https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto11.html