

David Carral -- Adán -- Nezha -- xabier

2º Sistemas Microinformáticos y Redes

Unidad: 4

Práctica Nº: 42

Título: Cifrados de la antiguedad

Fecha: 10/12/2025



Seguridad Informática

Índice

- David Carral -- Adán -- Nezha -- xabier
 - 2º Sistemas Microinformáticos y Redes
 - **Unidad: 4**
 - **Práctica Nº: 42**
 - **Título: Cifrados de la antiguedad**
 - **Fecha: 10/12/2025**
 - Índice
 - Método polibios:
 - cifrado cesar
 - ejemplo :
 - cifrado vigenere
 - ejemplo :

Lista de cifrados de la antiguedad y la edad media

1. playfair
2. método polibios
3. cifrado cesar
4. cifrado de vingenere

Metodo polibios:

Se trata de un cifrado trivial donde cada carácter se corresponde a una fila y columna de la matriz. Es un caso particular de un sistema de transposición monolalfabética por lo que un análisis de frecuencias sería más que suficiente para desvelar el mensaje oculto.

Los métodos de sustitución se basan en asignar a cada letra otro ente ,que puede ser también otra letra, o un número o un símbolo especial. La cifra de Polibio es históricamente la primera que emplea métodos de sustitución .

Para explicar el funcionamiento en castellano tenemos qye recurrir a un truco,debido a que en nuestro idioma se emplean más de 25 letras, cosa que en latín y griego no ocurre.

Para codificar un mensaje primeramente fromamos la siguiente tabla:

	A	B	C	D	E
A	a	b	c	d	e
B	f	g	h	i	j
C	k	l	m	n	o
D	p	r	s	t	u
E	v	w	x	y	z

La letra a se cifrará como AA, la b como AB,...Hemos eliminado la letra q, lo cual no redunda en el contenido del mensaje , siempre que sustituymos dicha letra por la k.Tampoco hemos incorporado la ñ porque se suele llevar mal con los ordenadores.

Ejemplo: Texto claro: cifrade polibio Texto cifrado: ACBDBADBAADAEDACECBDABBDC

Una de las ventajas del cifrado del polibio es que emplea únicamente 5 letras para escribir cualquier mensaje,y el problema que tiene es :el mensaje cifrado tiene el doble de longitud que el texto claro.

cifrado cesar

es un metodo simple de cifrado por sustitucion que reemplaza cada letra de un mensaje por otra que se encuentra un numero fijo de posiciones mas adelante o mas atras en el alfabeto

ejemplo :

texto plano: mensaje de ejemplo

texto cifrado:KHKVDMH GH HMHPOR

el ejemplo se hizo utilizando un desplazamiento de 3 letras mas adelante en el alfabeto

Original	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrado	d	e	f	g	h	i	j	k	l	m	n	o	p
Original	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrado	q	r	s	t	u	v	w	x	y	z	a	b	c

cifrado vegenere

es un metodo de cifrado polialfabetico que utiliza una palabra clave para cifrar un mensaje
funciona repitiendo la palabra clave hasta que tenga la misma longitud del mensaje cada letra
se cifra con una tabla de vegenere que es una tabla de 26 filas y 26 columnas donde cada fila
se desplaza un lugar respecto a la fila anterior

ejemplo :

texto plano : ejemplo

clave : vegenere

texto cifrado : ZNKZTCS

ENTRADA TEXTO PLANO																											
ENTRADA 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	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	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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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
		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