

# Ejercicios criptografía

## 1º: The flag is chinatown

En base a la foto proporcionada se puede deducir que hay que usar el metodo de cifrado de transposición china.



## 2º: discover\_hex\_morse\_code

Basandose en el enunciado se procede a decodificar el texto de hexadecimal.

**Pegue el texto que desea decodificar hexagonal aquí:**

```
2d 2e 2e 20 2e 2e 20 2e 2e 2e 20 2d 2e 2d 2e 20 2d 2d 2d 20 2e 2e 2e 2d 20 2e 20 2e 2d 2e 20 2e
2e 2d 2d 2e 2d 20 2e 2e 2e 2e 20 2e 20 2d 2e 2e 2d 20 2e 2e 2d 2d 2e 2d 20 2d 2d 2d 20
2e 2d 2e 20 2e 2e 2e 20 2e 20 2e 2e 2d 2d 2e 2d 20 2d 2e 2d 2e 20 2d 2d 2d 20 2d 2e 2e 20 2e
```

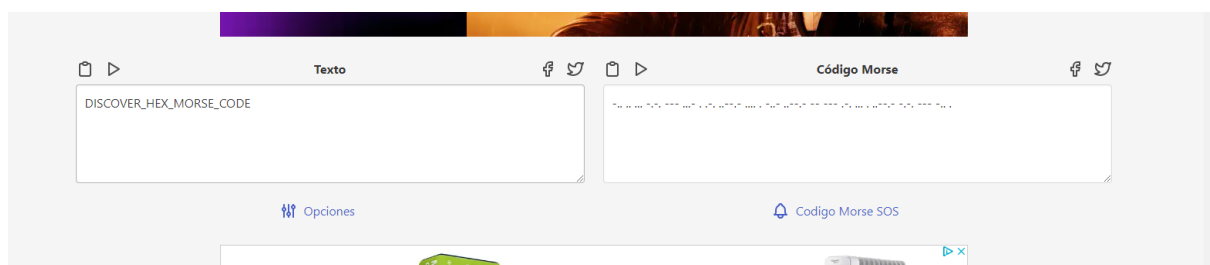
Hex al texto

[Descargar archivo](#)

**Copie el hexagonal decodificado texto aquí:**

```
.....
```

Podemos notar que el texto resultante es morse, asi que procedemos a convertirlo de nuevo.



### 3º: querer semejantes noticia sobre conocer misterio quien hizo

En base al enunciado, es tan sencillo como buscar las paginas, lineas y numero de palabra indicado.

Por ejemplo para la 10:8:2

---

#### CERVANTES

---

cuchillada, sacó su espada y le dió dos golpes, y con el primero y en un punto deshizo lo que había hecho en una semana; y no dejó de parecerle mal la facilidad con que la había hecho pedazos, y, por asegurarse deste peligro, la tornó a hacer de nuevo, poniéndole unas barras de hierro por de dentro, de tal manera, que él quedó satisfecho de su fortaleza y, sin **querer** hacer nueva experiencia della, la diputó y tuvo por celada finísima de encaje.

Fué luego a ver su rocín, y aunque tenía más cuartos que un real y más tachas que el caballo de Gonela, que *tantum pellis et ossa fuit*, le pareció que ni el Bucéfalo de Alejandro ni Babieca el del Cid con él se igualaban. Cuatro días se le pasaron en imaginar qué nombre le pondría; porque (según se decía él a sí mismo) no era razón que caballo de caballero tan famoso y tan bueno el por sí, estuviese sin nombre conocido; y así, procuraba acomodársele de manera, que declarase quién había sido antes que fuese de caballero andante, y lo que era entonces; pues estaba muy puesto en razón que, mudando su señor estado, mudase él también el nombre, y le cobrase famoso y de estruendo, como convenía a la nueva orden y al nuevo ejercicio que ya profesaba; y así, después de muchos nombres que formó, borró y quitó, añadió, deshizo y tornó a hacer en su memoria e imaginación, al fin le vino a llamar *Rocinante*, nombre, a su parecer, alto, sonoro y significativo de lo que había sido cuando fué rocín, antes de

Igual que para la 23:10:1 y así sucesivamente con el resto de paginas.



### CAPITULO III

DONDE SE CUENTA LA GRACIOSA MANERA QUE TUVO  
DON QUIJOTE EN ARMARSE CABALLERO

Y así, fatigado deste pensamiento, abrevió su venteril y limitada cena; la cual acabada, llamó al ventero y, encerrándose con él en la caballeriza, se hincó de rodillas ante él, diciéndole:

—No me levantaré jamás de donde estoy, valeroso caballero, fasta que la vuestra cortesía me otorgue un don que pedirle quiero, el cual redundará en alabanza vuestra y en pro del género humano.

El ventero, que vió a su huésped a sus pies y oyó semejantes razones, estaba confuso mirándole, sin saber qué hacerse ni decirle, y porfiaba con él que se levantase, y jamás quiso, hasta que le hubo de decir que él le otorgaba el don que le pedía.

—No esperaba yo menos de la gran magnificencia vuestra, señor mío —respondió don Quijote—; y así, os digo que el don que os he pedido y de vuestra liberalidad me ha sido otorgado es que mañana

4º:

El texto parec estar codificado en hexadecimal, y si probamos a decodificarlo vemos que el resultado esta en base64, asi que lo volvemos a decodificar desde base64.

hex

To Hex

From Hex

Hex to PEM

PEM to Hex

To Hexdump

From Hexdump

To Hex Content

From Hex Content

Hex Density chart

Parse ASN.1 hex string

Hex to Object Identifier

Recipe

From Hex

Delimiter  
Auto

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

Input

length: 440  
lines: 1

59556843656d517a545764684d303535a4735425a317074526e526a626d646e57544a61633249794e476461534842785a5564  
4e5a316b7a566a42615630316e596c684f4d5751795a32646156315a6f5a4668765a325674536e4e684d6e4e6e576d3543626d  
4e595157645a57454a74576a4a6e5a32517962486c684d30316e596c6857613246755a32645a5748426f597a4e725a316c5951  
6d356957456c6e59556477626c6c745557646c57484278595663775a324e496144466b6257396e5a56646f64574a745a326469  
563342785930646a5a32466e5054303d

Output

time: 3ms  
length: 121  
lines: 1

hpsws ksrvp famrx cflon dzjxc cutec msuwh eeauz zblkk fpgqp apfgh wirks mudjx azasy apgmr hjgbd yzjim  
pxuvj yhnnh mjjpg j

El resultado ya es texto sin caracteres raros, así que probamos a decodificarlo con la maquina enigma usando la informacion proporcionada en el enunciado

VIEW

Plaintext

hpsws ksrvp famrx cflon dzjxc cutec msuwh  
eeauz zblkk fpgqp apfgh wirks mudjx azasy  
apgmr hjgbd yzjim pxuvj yhnnh mjjpg j

ENCODE DECODE

Enigma machine

MODEL

Enigma M3

REFLECTOR

UKW B

ROTOR 1	POSITION	RING
I	- 1 A +	- 1 A +
ROTOR 2	POSITION	RING
II	- 2 B +	- 2 B +
ROTOR 3	POSITION	RING
III	- 3 C +	- 3 C +

PLUGBOARD

bq cr di ej kw mt os px uz gh

FOREIGN CHARS

Include Ignore

→ Decoded 121 chars

VIEW

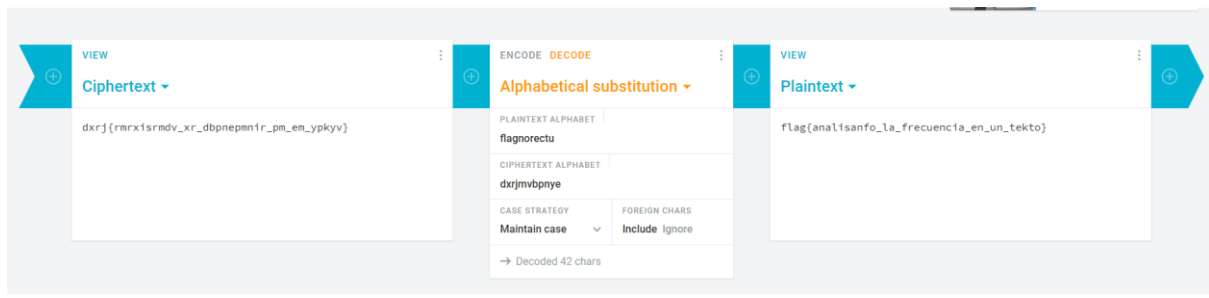
Text

ponga atenc ionsi fraca samos enest amis1  
onnos verem osabo cados aperd erlot odoan  
otees taban derae nigma mtres ukwbv i

“Ponga atencion si fracasamos en esta mision nos veremos abocados a perderlo todo ante esta bandera enigma m tres ukwbv j”

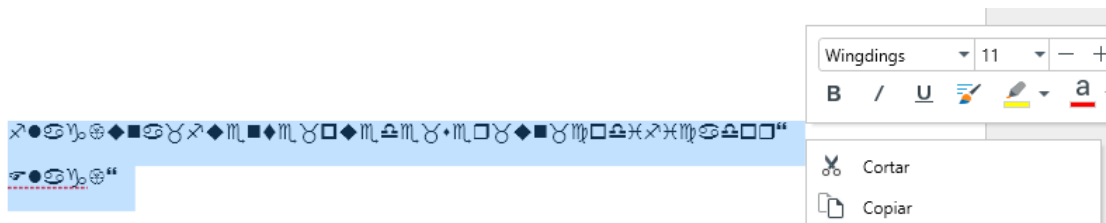
5º: flag{analizando\_la\_frecuencia\_en\_un\_texto}

Para este ejercicio hay que analizar la frecuencia de aparición de cada letra y buscar su homologa en español



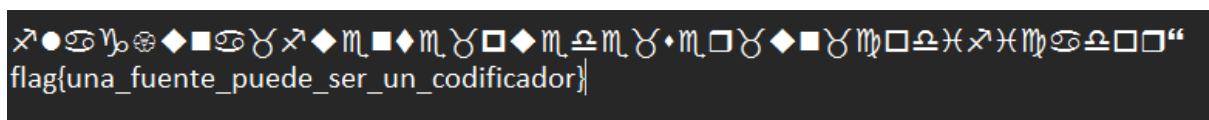
6º: flag{una\_fuente\_puede\_ser\_un\_codificador}

Si probamos a abrir el archivo en un editor de texto, vemos que la una fuente que admite esos caracteres es la wingdings



Asi que ahora solo hay que buscar sus homologos en ascii y listo

a	b	c	d	e	f	g	h	i	j	k	l	m	n
☪	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ
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
☪	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ
O	P	Q	R	S	T	U	V	W	X	Y	Z		
☪	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ
`	1	2	3	4	5	6	7	8	9	0	-	=	\
☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪
~	!	@	#	\$	%	^	&	*	(	)	_	+	
”	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪
[	]	{	}	;	‘	:	“	,	.	/	<	☪	☪
☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪	☪



7º: the flag is say we are crazy

Por la imagen se deduce que es cifrado en espejo, tambien llamado atbash. Asi que si decodificamos el texto este es el resultado

← → ↻ [pedrocarrasco.org/projects/criptografia/atbash.php?text=GSVUOZTRHHZBDVZIVXIZAB](https://pedrocarrasco.org/projects/criptografia/atbash.php?text=GSVUOZTRHHZBDVZIVXIZAB)

AulaVirtual Tutoriales de clase

### Este script (des)encripta un texto utilizando la técnica de atbash

Escribe el texto que quieres encriptar (solo a-z en minúsculas)

GSVUOZTRHHZBDVZIVXIZAB

Enviar

Texto a encriptar: GSVUOZTRHHZBDVZIVXIZAB  
Texto encriptado: theflagissaywearecrazy

---

El proceso de (de)codificación se realiza mediante la sustitución de la posición que ocupa en el abecedario cada uno de los caracteres en - Tabla de intercambio de caracteres. Los caracteres de arriba se sustituyen por los de abajo para cifrar el texto:

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

La sustitución es directa, es decir, la a => z, b => y, etc...

[Decodificar](#) el texto sigue el mismo proceso

[codificar mediante transposicion](#) | [codificar mediante sustitucion](#) | [codificar mediante albam](#) | [codificar mediante atbah](#)

---

Pedro Carrasco © 9 Marzo 2010

8º: flag{estamos\_empezando\_a\_conocer\_algo\_de\_historia}

La referencia a Julio Cesar nos da la pista de que hay que usar el cifrado del cesar.

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:  
e.g. type 'boolean'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

Brute-Force mode: the 25 shifts (for the alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ) are tested and sorted from most probable to least probable.

↑↓	↑↓
11	11
la siguiente informacion es confidencial. Te ayudara a proseguir en la investigacion. No te confies, no todas las informaciones de las que disponemos son tan faciles como esta	
3) rotacion de caracteres. Firmado: un amigo.	
flag{estamos_empezando_a_conocer_algo_de_historia}	

Cryptography › Substitution Cipher › Caesar Cipher

### CAESAR CIPHER DECODER

★ CAESAR SHIFTED CIPHERTEXT (?)

yn fvthvragr vasbeznpvba rf pbasvqrapvny. Gr nlhqnen n cebfrthve ra yn vairfgvtnpvba. Ab gr pbasvrf, ab gbqnf ynf vasbeznpvbarf qr ynf dhr qvfcbazbf fba gna snpyvrf pbzb rfgn ebgnpvba qr pnenpgrrerf. Sveznqb: ha nzvtb. synt{rfgnzbf\_rzcrmqnb\_npbabpre\_nytr\_qr\_uvfgbevn}

Test all possible shifts (26-letter alphabet A-Z)

► DECRYPT (BRUTEFORCE)

#### MANUAL DECRYPTION AND PARAMETERS

★ SHIFT/KEY (NUMBER): 3

☒ USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)

☐ USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9

☐ USE THE LATIN ALPHABET IN THE TIME OF CAESAR (23 LETTERS, NO J, U OR W)

☐ USE THE ASCII TABLE (0-127) AS ALPHABET

☐ USE A CUSTOM ALPHABET (A-Z0-9 CHARS ONLY)

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ

9º: the flag is mareados

La imagen de la ruta 66 nos da la pista de que hay que usar un cifrado por transposicion de 7x7 y el tornado es la forma de leer las letras en espiral .

H	I	C	I	M	O	S
N	C	R	E	I	B	L
I	S	S	M	A	L	A
E	I	O	S	R	E	R
U	G	D	A	E	T	U
F	A	L	F	E	H	T
O	T	O	M	N	E	A

10º: 4458256

Lo que hay que hacer en este ejercicio es utilizar un decodificador de imagen SSTV para extraer el texto oculto en el audio.

