

# Esteganografía

## Parte 1: Conocimiento Previo

CC5325 - Taller de Hacking Competitivo

# Codificaciones

- En general, 8 bits hacen un byte
  - Un byte puede representar 256 valores diferentes
- Bytes se suelen representar en
  - Binario (8 dígitos)
  - Octal (3 dígitos)
  - Hexadecimal (2 dígitos)
- ¿Cómo represento texto con bytes?
  - Estándares como ASCII o ISO8859-1
    - 1 byte = 1 caracter.

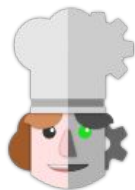
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
1	0	1	0	0	0	1	1

$8^2$   $8^1$   $8^0$

2	0	5
---	---	---

$16^1$   $16^0$

1	0
---	---



<https://gchq.github.io/CyberChef/> {From,To} {Decimal,Octal,Hex}

# Codificaciones

---

- Codificaciones comunes para datos binarios
  - Base64 (y Base58 y Base32):
    - Cada caracter representa un conjunto de bits:
      - Base64: 6 bits por caracter
      - Base32: 3 bits por caracter
      - Base58: un poco menos de 6 bits por caracter.
    - Permiten transmitir datos binarios arbitrarios en un canal que soporta datos alfanuméricos (o ASCII) solamente.



<https://gchq.github.io/CyberChef/>

{From,To} Base{32,58,62,64,85}

# Esolangs

---



**Piet**

```
+++++++ [ >++++++>++++  
+++++>+++>+<<<<- ]>+ .>+  
.+++++. .+++ .>+ .<<++++  
+++++++ .> .+++ .-----  
.----- .>+ .> .
```

**Brainf\*ck**

<https://gist.github.com/eriverosr/bb4e39ff91879bd30bb9d6417cd9057f>

???

# Ofuscación de Código

— — —

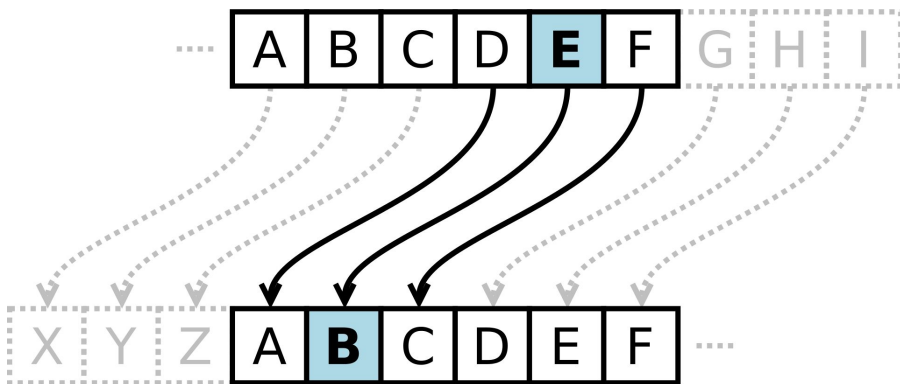
```
var
_0xb12b=["\x53\x61\x6C\x75\x64\x61","\x43\x43\x35\x33\x
32\x35\x7B\x30\x66\x75\x35\x63\x34\x63\x31\x30\x6E\x5F\x
6A\x34\x76\x34\x35\x63\x72\x31\x70\x74\x7D","\x68\x6F\x
6C\x61\x2C\x20","\x47\x65\x74\x43\x6F\x75\x6E\x74","\x
45\x73\x74\x61\x20\x6E\x6F\x20\x65\x73\x20\x6C\x61\x20\x
66\x6C\x61\x67\x2E"];function
NuevoCofre(){this[_0xb12b[0]]=function(_0xb3cbx2){var
_0xb3cbx3=_0xb12b[1];alert(_0xb12b[2]+
_0xb3cbx2)};this[_0xb12b[3]]=function(){return
count}}var obj=new NuevoCofre();obj.Saluda(_0xb12b[4])
```

¿Qué hay acá?

<https://gist.github.com/eriverosr/b12f66e5ae6e6c254f4ece488d982094>

# Criptografía Clásica: Caesar

---  
K = 3 (o C)



fr qvpr dhr whyvb prfne hfnon  
rfgr pvsenqb cnen raivne fh  
pbeerfcbaqrapvn cevinqn



<https://www.dcode.fr/caesar-cipher>

# Criptografía Clásica: Vigenere

---

**K=GATO= 6 0 19 14**

C	O	M	P	R	A	P	A	N	E	N	L	A	T	A	R	D	E
G	A	T	O	G	A	T	O	G	A	T	O	G	A	T	O	G	A
I	O	F	D	X	A	I	O	T	E	G	Z	G	T	T	F	J	E

YVVKCBOOYVVHPRSVNQYLRTPSXHYTRBBSASITLRKBJRZLAHRSWGVPZDKYTRMDSZBZOCKOSNGWHPT  
JRBVPBRBOVJFVBRPEZQWELRTJHQMUBQTLDJOITLWXSWSGEYVARGMJHKXPVNBXXTXJATFVUGSWFWSRG  
BBJSCDCBATXZJHYXPXEGFBFMFXNHMSFKWPDWHVJMYMAGYVRMRAEGMOJTJKAOIMYTNIABJR



<https://www.dcode.fr/cifrado-vigenere>

# Criptografía Clásica: Sustitución Monoalfabética

---

**Cifrado:** Reemplazar letras de arriba por letras de abajo

**Descifrado:** Reemplazar letras de abajo por letras de arriba

¿Cómo conozco el alfabeto de sustitución?

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

<https://gist.github.com/eriverosr/5f9da031b82bd2c6844ce933476ffb40>

Herramienta: <https://cryptii.com/pipes/alphabetical-substitution>