Curso CTF Competitivo

Presentación: Antonio González Pardo e Isaac Lozano Osorio

Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

Índice

Horario y aula de clase

- 30 Septiembre – 16 Diciembre
- Todos los viernes de **17:00 a 19:00**
- **Presencial**: Se anunciará el aula por **correo cada semana y si no la web estará actualizada.**
- Información: https://urjc-ctf.github.io/web/
- Recomendado asistir a todas las sesiones. Solo se realizarán presencial y sin grabaciones, si te pierdes alguna tienes la grabación del año anterior.

Material básico necesario

¿Qué es necesario para participar?

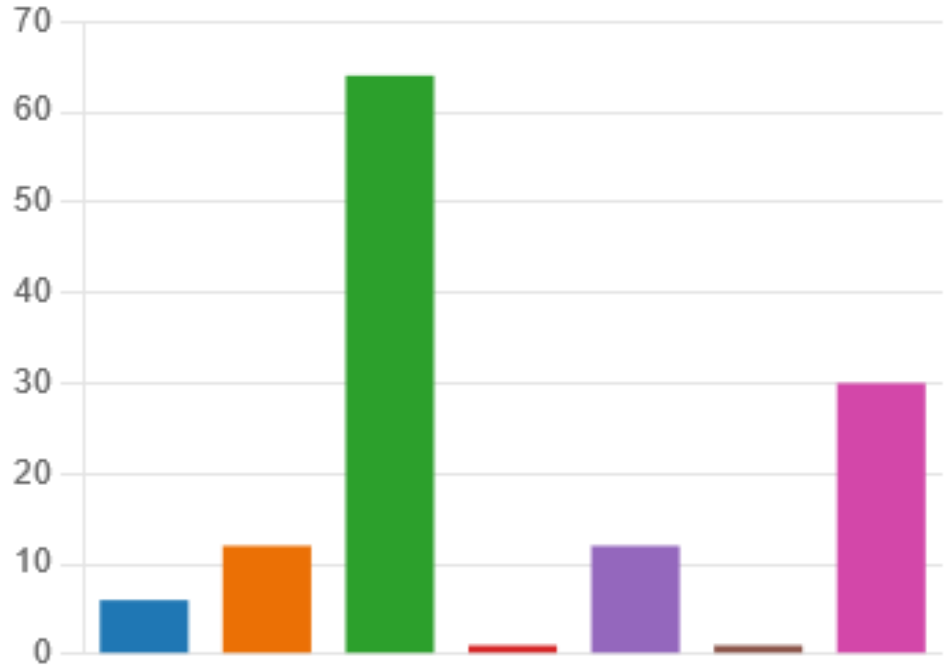
- Un ordenador con conexión a internet (obviamente)
- VirtualBox, para usar la imagen que os vamos a proporcionar
- Ganas de aprender
- Recomendado:
  - Conocimientos básicos en algún lenguaje de programación
  - Conocimientos básicos de Linux y/o terminal
  - Soltura utilizando los buscadores (Google, Bing, DuckDuckGo…)

Universidad Rey Juan Carlos

¿Quiénes sois vosotros?

Grado en el que estás matriculado (u otros estudios)

Software	6
Informática	12
Ciberseguridad	64
Matemáticas	1
Computadores	12
Videojuegos	1
Otras	30



¿Quiénes sois vosotros?

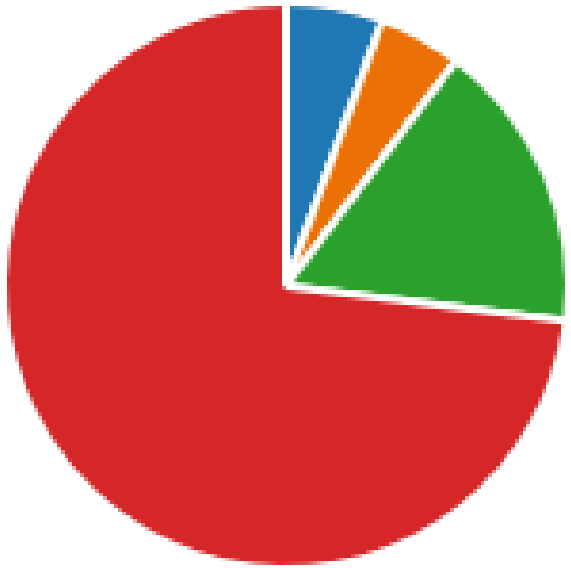
Curso en el que estás matriculado

1º	65
2º	32
3º	14
4º	9
Otras	6

¿Quiénes sois vosotros?

¿Has participado antes en CTFs?

Sí, participo de forma frecuente ...	7
Ocasionalmente (1 al mes, o cad...	6
Alguna vez (1-2 al año)	21
Nunca he participado en un CTF.	92



Universidad Rey Juan Carlos

Módulos del curso

Módulo I: Introducción a retos básicos, criptografía

Módulo II: OSINT, Forense y Esteganografía

Módulo III: Ataques a servidores y explotación web

Módulo IV: Reversing y explotación de binarios

Universidad Rey Juan Carlos

Personas que han cursado el curso

1. **Nuevo contenido**
2. **Nuevos retos (facilidad en algunas asignaturas de la carrera el realizarlos)**

Universidad Rey Juan Carlos

Plataforma de retos del curso

https://ctf-curso.numa.host/

Credenciales en correo de bienvenida

Universidad Rey Juan Carlos

Plataformas recomendadas

Pico CTF: https://picoctf.org/

OverTheWire: https://overthewire.org/wargames/

TryHackMe: https://tryhackme.com/

HackTheBox: https://www.hackthebox.eu/

Atenea: https://atenea.ccn-cert.cni.es/home

Créditos RAC

Asistencia mínima de **10 clases** y **registrado** en el control de asistencia de la aplicación de la URJC.

Créditos: 1,25 ECTS

Universidad Rey Juan Carlos

¿Cómo interactuar?

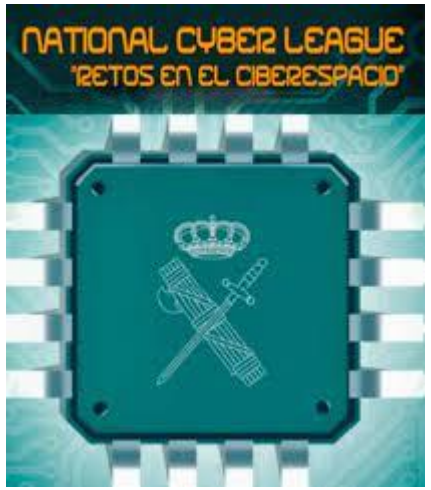
Levantamos manos.

Somos un equipo numeroso y para los retos se pueden preguntar dudas y se irá a cada ordenador a solucionarlas.

El propósito es aprender, no solo competir.

Y responder al correo en copia a todos, en otro caso os reviento

Experiencia de los Docentes



Facebook Bug Bounty

BIT UP

SEEK & HACK

Qynamon

HackOn 2022

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

JNIC Jornadas Nacionales de Investigación en Ciberseguridad

EUROPEAN CYBER SECURITY CHALLENGE

grafo RESEARCH

Universidad Rey Juan Carlos

1. Introducción a los CTF y criptografía básica

Carlos Alonso, Pablo Pastor, Inés Martín

Universidad Rey Juan Carlos

Universidad Rey Juan Carlos

Índice

1. ¿Qué es un CTF?
2. ¿Qué tipos de retos se encuentran en los CTF?
3. Conceptos básicos: encuentra la bandera
4. Criptografía y codificaciones básicas
   - Representación de los datos
   - Codificaciones y cifrados
   - Otros cifrados (XOR, Dcodefr…)
   - Hashes (MD5, SHA1, SHA256)
5. Retos básicos

¿Qué es un CTF?

Universidad
Rey Juan Carlos

¿Qué es un CTF?

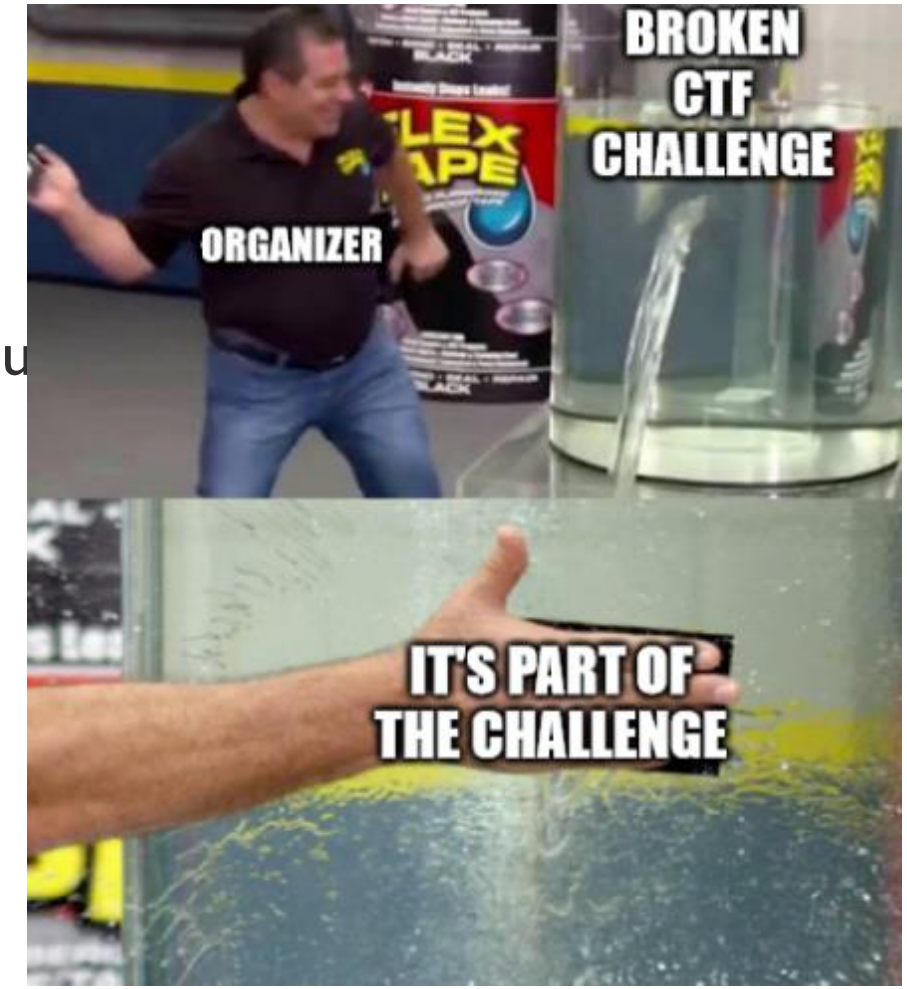
CTF = Capture The Flag (Captura la Bandera)

- Competición de **hacking**, en la que ponemos a prueba nuestras **habilidades resolviendo retos de ciberseguridad** en un **tiempo limitado**, con el objetivo de sumar puntos**.**
- Por **equipos o individual**

Conceptos básicos: encuentra la bandera

1. **Elige** un reto
2. **Resuélvelo** lo antes posible
3. **Introduce la flag** y obtén pu

```
N=340406247493724286139524398114141837754919074919 3
e = 2^16 + 1
069964742448854721353801868728817946899740624652 9 #
160289500416284268111465338714710278910245340416 3 #
209483623565439572745858942993342570484788373108 5 #
175060718655970371385193307720798342022353251906 2
```



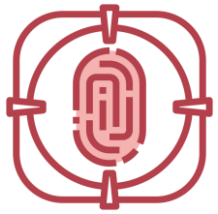

```
$ ./decrypt.py
Onk.Onk.Onk.Onk.Onk.
OnkHackOn{G00se_Game
}Onk.Onk.OnkOnk.Onk.
OnkOnk.Onk
```

Tipos de CTF

Existen **3 tipos principales** de competiciones CTF:

1. **Jeopardy**: retos de **distintas categorías** a resolver en un **tiempo limitado**.
2. **Ataque – Defensa**: **2 equipos, 2 redes** y **servicios vulnerables** en cada red. Ambos equipos deben **atacar a los servicios del contrincante** a la vez que **defienden los suyos.**
3. **Boot2root**: **máquinas** creadas **con fallos** de seguridad que se deben **explotar** para convertirse **en superusuario *(root)*.**
4. **Mezcla**

Categorías



Forense

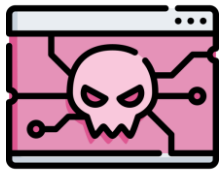
Investigaciones sobre incidentes informáticos

Web

Búsqueda y explotación de vulnerabilidades en aplicaciones web

Criptografía

Descifrado de mensajes ilegibles a simple vista



Reversing

Análisis del código de programas y ejecutables

OSINT

Recolección de datos a través de fuentes públicas de información

Esteganografía

Técnica que oculta mensajes o archivos dentro de otros

CRIPTOGRAFÍA BÁSICA

Universidad
Rey Juan Carlos

Criptografía - Representación de los datos

Es esencial entender que **nos podemos encontrar los datos con diferentes formatos**. Sin embargo, **su significado será el mismo**. Las formas más comunes son:

ASCII

Relaciona caracteres con números. A cada carácter le corresponde un valor de la tabla ASCII.

ASCII	Símbolo
96	`
97	a
98	b
99	c
100	d
101	e
102	f
103	g
104	h
105	i
106	j
107	k
108	l
109	m
110	n
111	o

Hexadecimal

Utiliza base 16 como representación de los datos. En caracteres toma como referencia el valor ASCII

Criptografía - Representación de los datos

Es esencial entender que **nos podemos encontrar los datos con diferentes formatos**. Sin embargo, **su significado será el mismo**. Las formas más comunes son:

Binario

Es la representación más básica. Tan solo utiliza dos valores: 1 y 0.

DECIMAL	BINARIO	HEXADECIMAL
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Palabra

CTF{Bienvenidos}

ASCII

067 084 070 123
066 105 101 110
118 101 110 105
100 111 115 125

Binario

01000011 01010100 01000110
01111011 01000010 01101001
01100101 01101110 01110110
01100101 01101110 01101001
01100100 01101111 01110011
01111101

Hexadecimal

43 54 46 7b 42 69 65 6e
76 65 6e 69 64 6f 73 7d e2
80 8b

CyberChef: https://gchq.github.io/CyberChef/
Dcode.fr: https://www.dcode.fr/

Universidad Rey Juan Carlos

Criptografía - Codificaciones y cifrados

Algunas de las maneras más comunes de ocultar información son mediante **codificaciones y cifrados**. Esto consiste en utilizar una única clave para cifrar y descifrar la información. Por lo tanto, siendo el cifrado **reversible**.

Codificaciones

- Representan la misma información de diferentes maneras.
- Es reversible
- Algunos ejemplos son Base64, Base32 o ASCII

Cifrados

- Ocultan la información mediante claves, normalmente secretas, y un conjunto de operaciones.
- Es reversible
- Algunos ejemplos son ROT-N/César o Vigenère

Criptografía - Codificaciones y cifrados

BASE64

Es un sistema de **numeración posicional** que usa 64 caracteres como base.
Sirve para representar cualquier información en binario como texto. **Se suele identificar rápidamente** por su estructura (en general, suelen acabar en ==)

Texto original

CTF{Esto es un texto en Base64. También existen otras como Base32, Base58 o Base85, por ejemplo}

Texto en Base64

Q1RGe0VzdG8gZXMgdW4gdGV4dG8gZW4gYXNlNjQuIFRhbWJp6W4gZXhpc3RlbiBvdHJhcyBjb21vIEJhc2UzMiwgQmFzZTU4IG8gQmFzZTg1LCBwb3IgZWplbXBsb30=

Criptografía - Codificaciones y cifrados

ROT-N

Es un tipo particular de cifrado en el que los caracteres se desplazan N posiciones. Por ello, N será nuestra clave secreta que ayudará a cifrar y descifrar el texto. Además de conocer la clave, deberemos conocer el diccionario que se usa.

Texto original

CTF{El rot solo va a modificar las letras, pero no las llaves}

abcdefghijklmnopqrstuvwxyz

Texto en ROT 13

PGS{Ry ebg fbyb in n zbqvsvpne ynf yrgenf, creb ab ynf yynirf}

nopqrstuvwxyzabcdefghijklm

Cifrado de César

Criptografía - Codificaciones y cifrados

Vigenère

Se basa en una **tabla con dos entradas.** Una será **la clave** y la otra **el texto a cifrar**. Iremos sustituyendo en el texto carácter a carácter con ayuda de la tabla y la clave. La clave será la misma para cifrar y descifrar.

Texto original

CTF{Mi clave de cifrado es Chachipiruli}

Texto en Vigenère

EAF{Op kaimy om epfthld mj Wsieoirpzjtz}

Criptografía - Codificaciones y cifrados

ENTRADA CLAVE \ ENTRADA TEXTO PLANO	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

C T F { M i c l a v e d e c i f r a d o e s C h a c h i p i r u l i }
C H A { c h i p i r u l i C h a c h i p i r u l i C h a c h i p i r l }
E A F{O p k a i m y o m e p f t h l d m j W s i e o i r p z j t z}

Texto original

CTF{Mi clave de cifrado es Chachipiruli}

Texto en Vigenère

EAF{Op kaimy om epfthld mj Wsieoirpzjtz}

Criptografía - Otros cifrados

XOR

Consiste en cifrar siguiendo unas **reglas matemáticas** y una **clave secreta**. Como la **longitud** de la **clave** suele ser **menor al texto**, se repetirá **cíclicamente**. Todos los caracteres se pasarán a binario y se operará con ellos. Reglas:

1. **Conmutativa:** `A xor B = B xor A`
2. **Asociativa:** `(A xor B) xor C = A xor (B xor C)`
3. **Autoinversa:** `(A xor B) xor B = A`

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

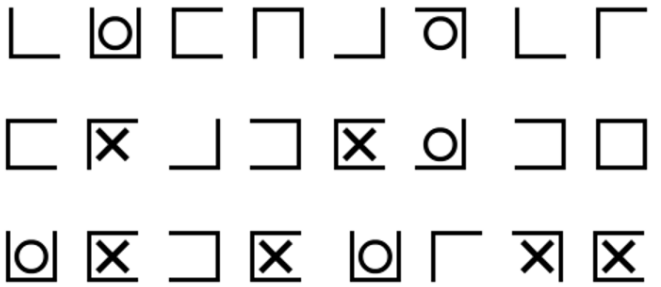
Criptografía - Otras codificaciones

Tic-Tac-Toe

Texto original

CTF{Hay cifrados de todo tipo}

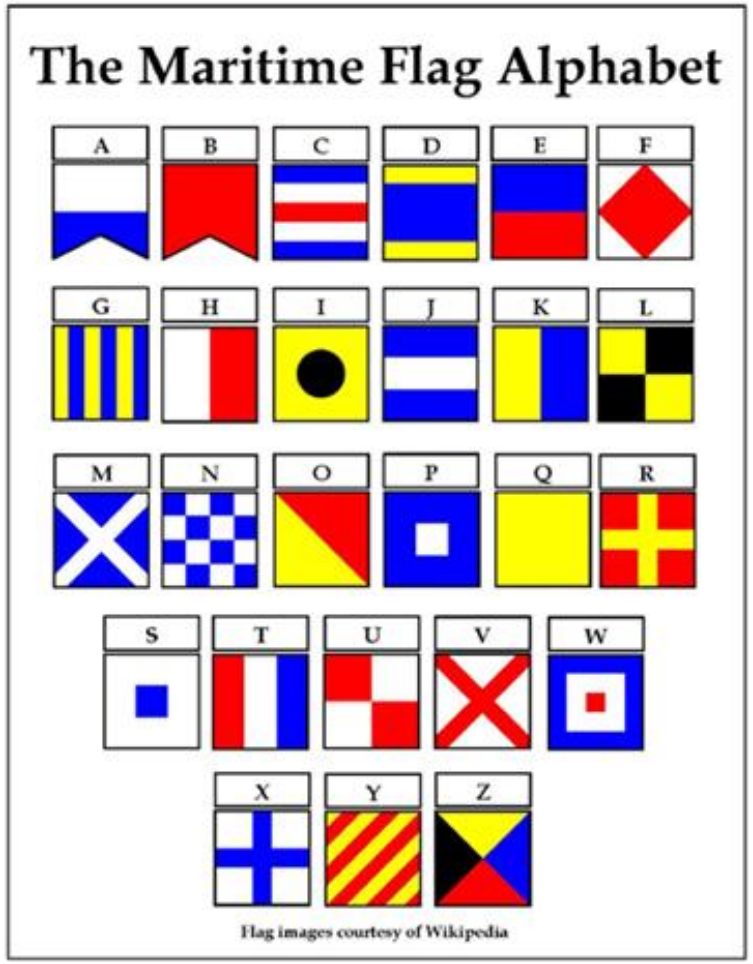
Texto en Tic-Tac-Toe



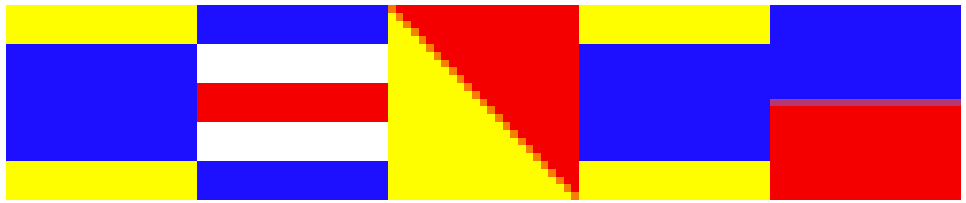
DCode.fr: https://www.dcode.fr/chiffre-tic-tac-toe

Criptografía – Otras codificaciones

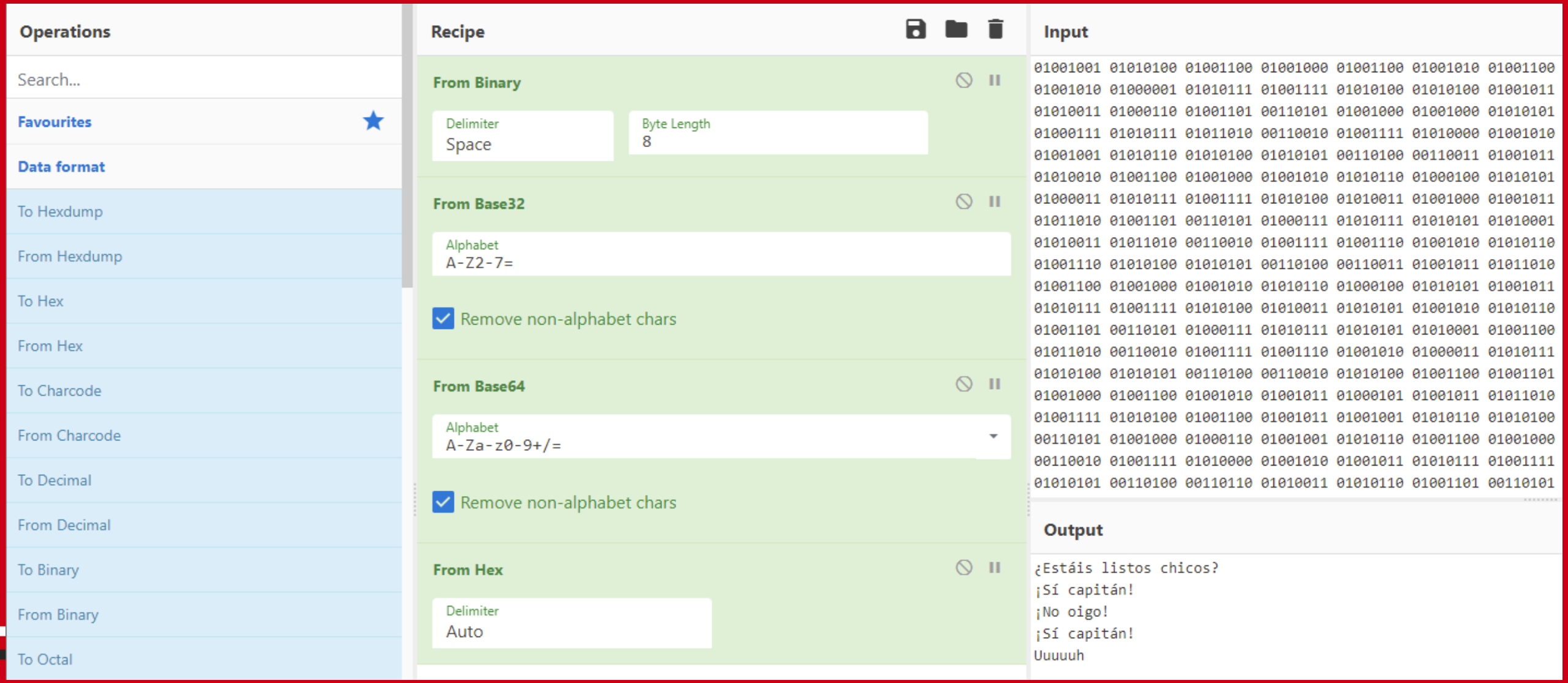
Sustitución con Banderas marítimas



Texto original: DCODE



https://www.dcode.fr/maritime-signals-code



Universidad Rey Juan Carlos

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

EJ 1: VVJKQ3tNdXkgYmllbiwgdmVvIHF1ZSBzYWJlcyBpZGVudGlmaWNhciB1biBiYXNlNjR9

EJ 2: YVNG{Rs xshsw psw VSX wsr 57}

EJ 3.
Vm0wd2VFNUdiRmRVV0doVlYwZG9WRll3YUVOamJGWnpWbTVrVkUxV1ZqTldNalZyWVdzeFdGVn
NXbFpOYm1oeVdXdGtSbVZYVmtaaVlwWlhWakpvYjFkV1kzaFdNVnB6Vkd4c1lWSnRhSEJWYWtwdlR
XeGFSMVp0ZEZSaVZscDZWbGQ0YjFsV1NYZFhiR3hXWWtaS1ZGUlVSbHBsUm1SMFkwVTFVMkpVY
XpCWFZsSlBZekpHVjFOcVdsTmlhMXBoV1d0YVlXRkdhM2xsU0U1cVZteEtlVlJzWkVkVWJVVjZVV3h3
VjFaNlFYaGFSRVpQWXpGT1dXRkdVbWxoZWxaV1ZtMTRhMkl4WkVkaIJXUllZbXMxV0ZWdGRHRm
xSbFY1VFZWa1dGSnJOVWRWYkZKR1VGRTIQUT09

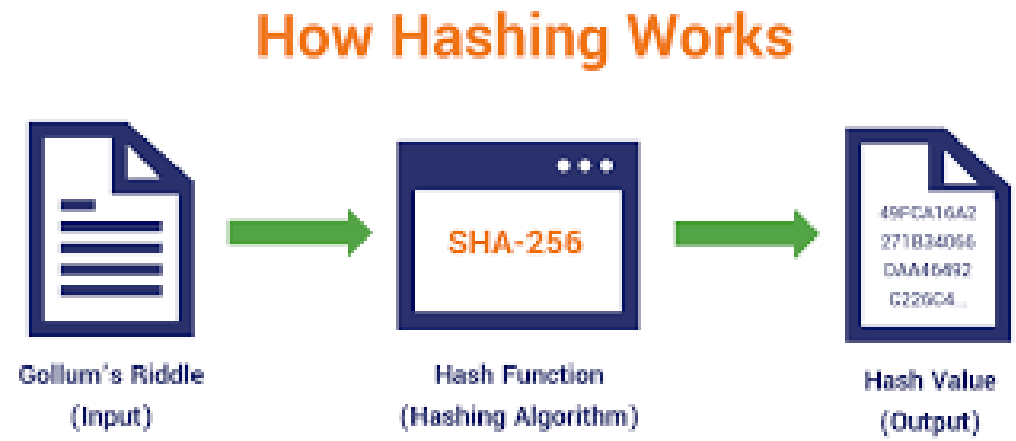
EJ 4: ..- .-. .--- -.-. { . ... - --- . ... -.-. --- -.. .. --. --- -- --- .-. ... . }

Ejercicios propuestos

Criptografía - Hashes

¿Qué es un hash?

- Es una **función matemática o criptográfica**, resume la información
- Da como **resultado** una cadena de caracteres de longitud fija (***digest***), **independientemente** de la longitud entrada
- Es **irreversible**. Una vez aplicada **no se puede obtener el valor inicial.**

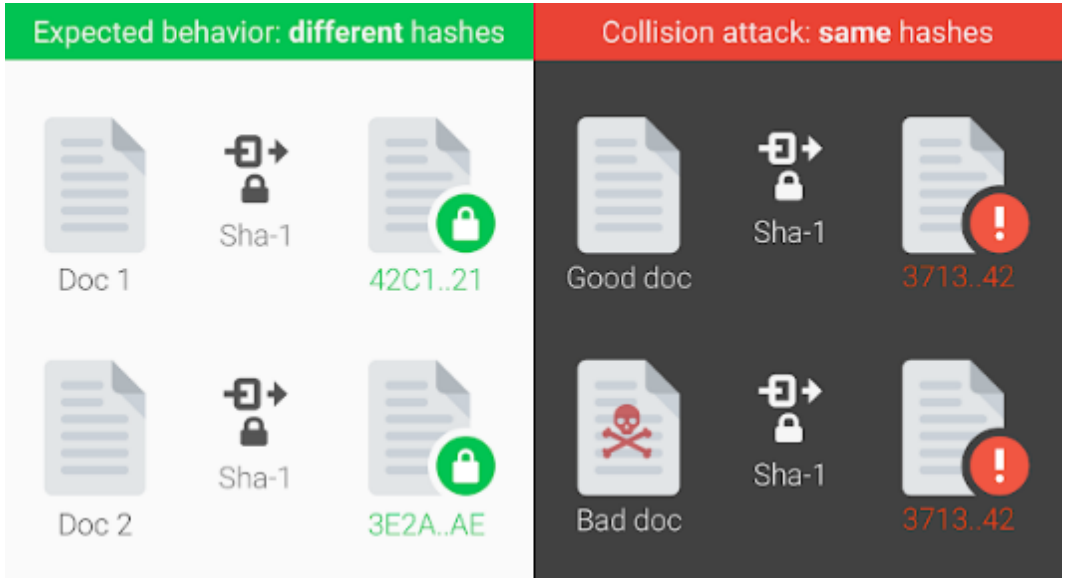


Criptografía - Hashes

- Lo que sí puede hacerse es **pre-computar** cadenas típicas, dado que una función hash devolverá el mismo resultado para la misma cadena (es determinista)
- **Conociendo la función utilizada** podemos realizar ataques de **fuerza bruta** sobre los hashes, de forma que, si en nuestro **diccionario** se encuentra la palabra *hasheada*, **sabremos qué esconde el hash**
- Es importante destacar que esto **NO ES LO MISMO QUE REVERTIR EL CÁLCULO**
- **Intentar adivinar un hash** de una palabra de longitud mayor que 8 es **computacionalmente muy costoso**

Criptografía - Hashes

- Existen determinadas funciones hash cuyo uso **no se recomienda**
  - **MD5**
  - **SHA1**
- Aunque la probabilidad es muy baja, podrían existir **colisiones**

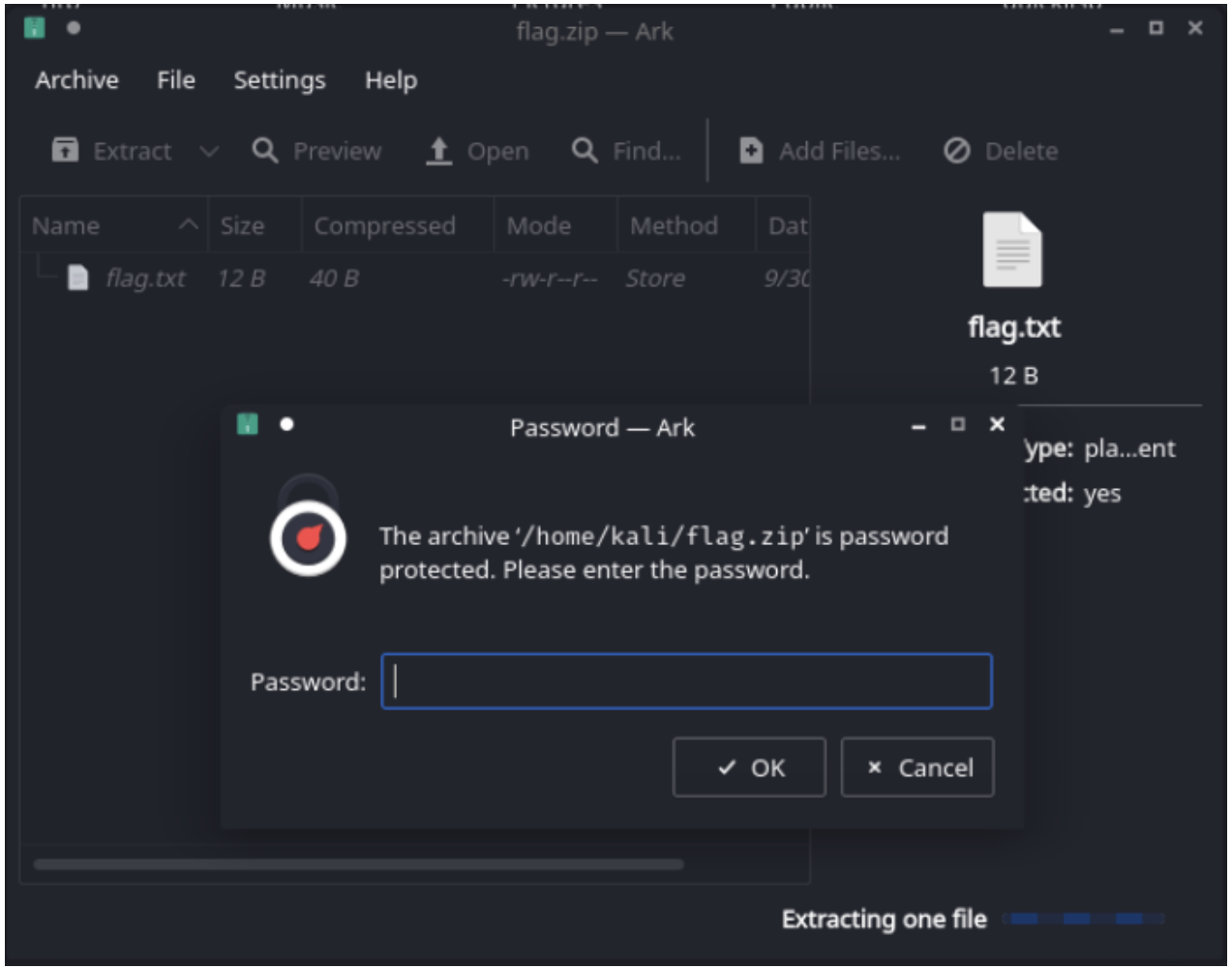


Criptografía - Hashes

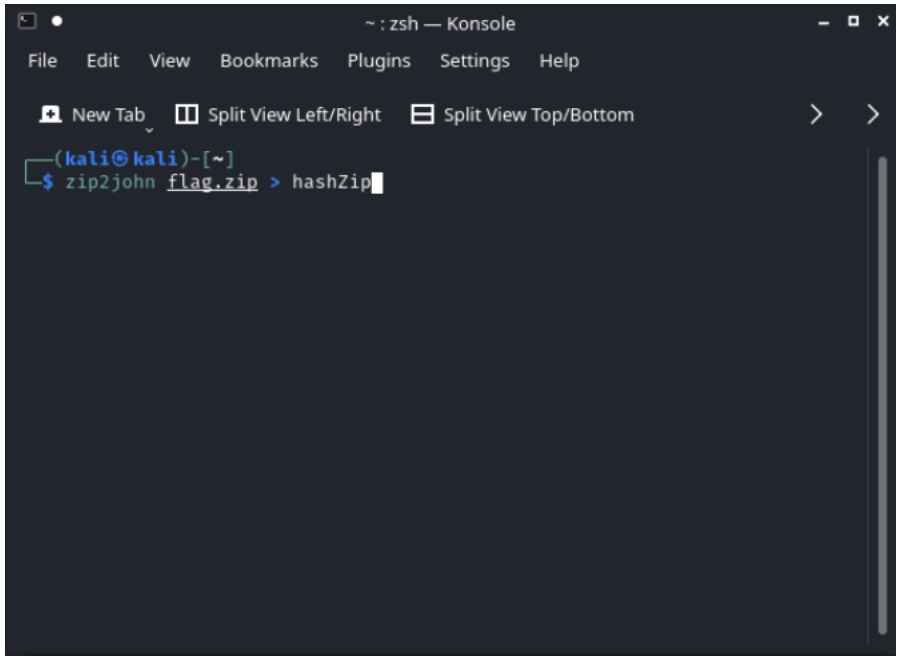
- Cada **fichero** se puede resumir con un **valor hash**
- Existen herramientas que, dada una lista de **hashes,** nos automatizan el proceso de obtener un valor que genere dicho hash.
- **Esto permite obtener la contraseña de ficheros cifrados**

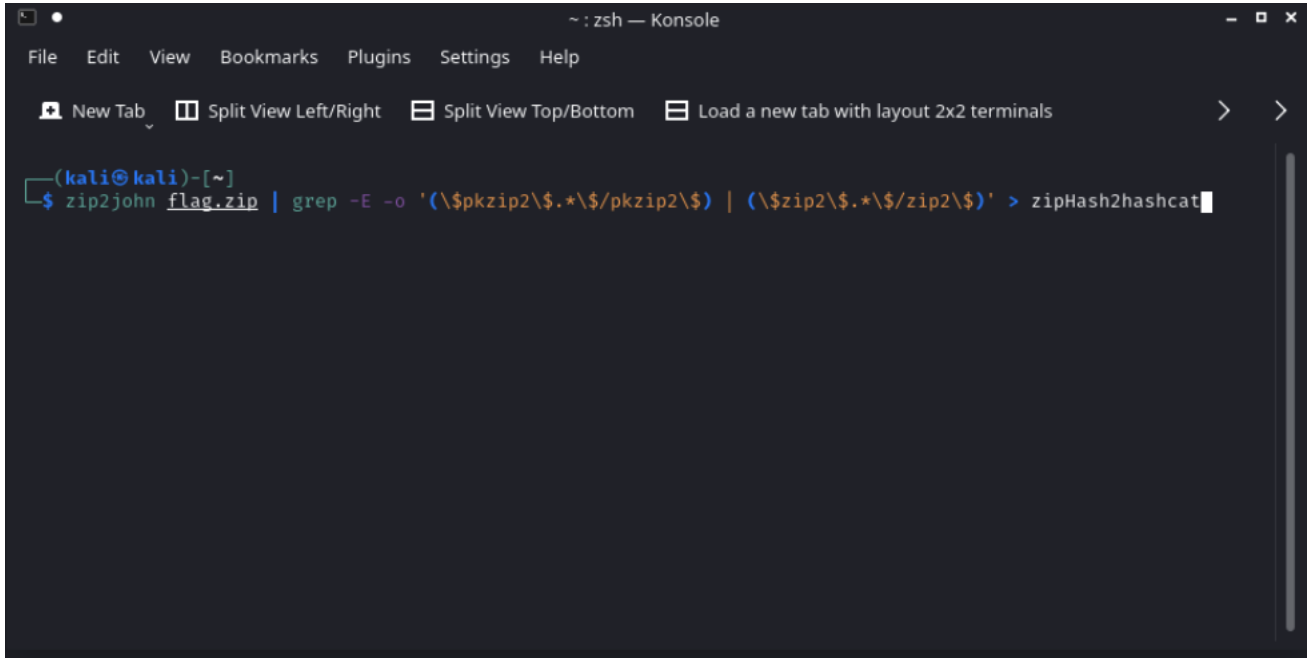
Universidad Rey Juan Carlos

Criptografía – Hashes (Ejemplo)

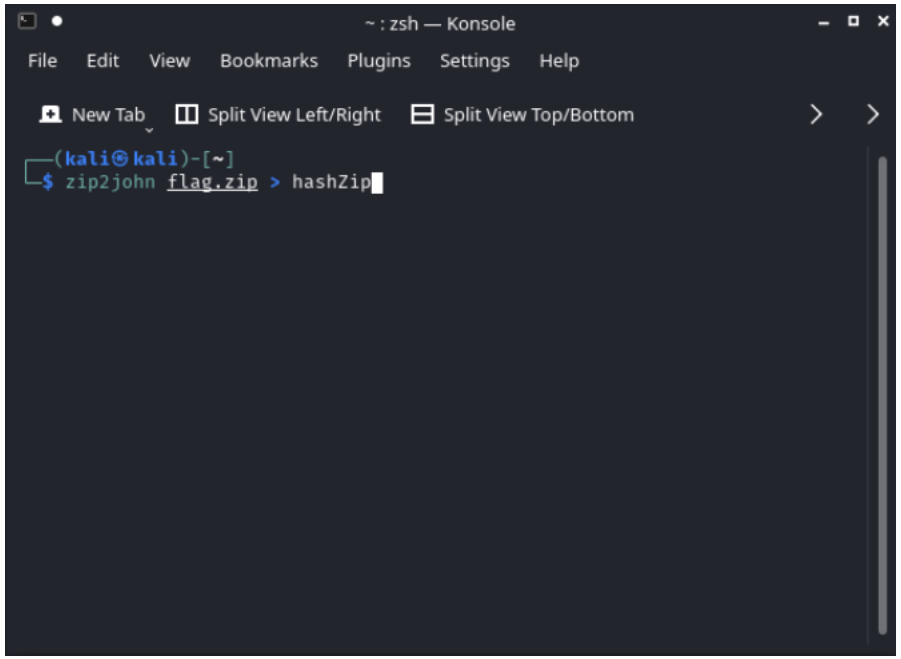


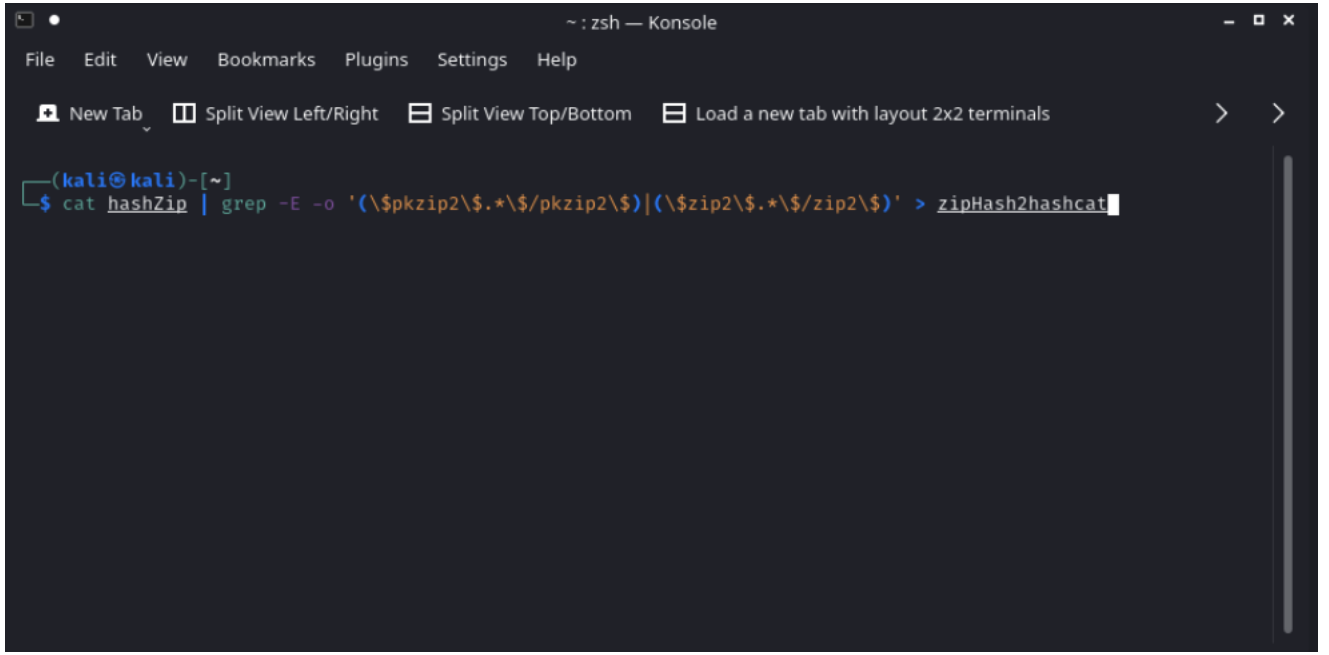
Criptografía – Hashes (Ejemplo)





Criptografía – Hashes (Ejemplo)





Criptografía – Hashes (Ejemplo)


```
~ : zsh — Konsole
File  Edit  View  Bookmarks  Plugins  Settings  Help
New Tab  Split View Left/Right  Split View Top/Bottom

┌──(kali㉿kali)-[~]
└─$ john hashZip --wordlist=wordlists.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 16 needed for performance.
hola1234         (flag.zip/flag.txt)
1g 0:00:00:00 DONE (2021-09-30 16:55) 100.0g/s 100.0p/s 100.0c/s 100.0C/s hola1234
Use the "--show" option to display all of the cracked passwords reliably
Session completed

┌──(kali㉿kali)-[~]
└─$ john hashZip --show
flag.zip/flag.txt:hola1234:flag.txt:flag.zip:flag.zip

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 13600 zipHash2hashcat ./wordlists.txt
hashcat (v6.1.1) starting ...

Session..........: hashcat
Status...........: Cracked
Hash.Name........: WinZip
Hash.Target......: $zip2$*0*3*0*f819c01513f1f5018f4e73128d711b52*8d6c* ... /zip2$
Time.Started.....: Thu Sep 30 16:59:35 2021 (0 secs)
Time.Estimated...: Thu Sep 30 16:59:35 2021 (0 secs)
Guess.Base.......: File (./wordlists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:        3 H/s (1.66ms) @ Accel:64 Loops:999 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 1/1 (100.00%)
Rejected.........: 0/1 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-999
Candidates.#1....: hola1234 -> hola1234

Started: Thu Sep 30 16:58:55 2021
Stopped: Thu Sep 30 16:59:37 2021

┌──(kali㉿kali)-[~]
└─$ hashcat -m 13600 zipHash2hashcat --show
$zip2$*0*3*0*f819c01513f1f5018f4e73128d711b52*8d6c*c*327662bd488eec34fe3ad3fa*4b36073395bdba927dda*$/zip2$:hola1234

┌──(kali㉿kali)-[~]
└─$
```

Criptografía - Hashes

- Como **atacantes**, esto nos viene bastante bien, dado que **podemos intentar encontrar colisiones que nos favorezcan**

- Como **defensores**, debemos utilizar siempre **funciones hash seguras**

RETOS BÁSICOS

Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

Para practicar lo aprendido

- Para **practicar lo que hemos visto hasta ahora**, podéis realizar los **primeros 7 retos** de la categoría ***Básica*** de la plataforma **Atenea**

https://atenea.ccn-cert.cni.es/challenges

- Estos retos resumen **lo visto hasta ahora**
- La semana que viene, veremos **criptografía más avanzada**
  - **RSA, AES, etc.**

1. Introducción a los CTF y retos básicos

Inés Martín, Carlos Alonso y Pablo Pastor

Universidad
Rey Juan Carlos