InTr0 a los CTF: ¿S4b3s d3sc1fr4r 3l m3ns4j3 0cult0? - Taller de crypto

HACKMADRID %27

Eventos HackMadrid%27

Eventos de FEBRERO

27/02 - 20:00 horas - HackMeetingOnline
<Una aproximación a la seguridad de Kubernetes>
Presenta: Rod Soto

HACKMADRID %27

Eventos de MARZO

03/03 - 18:30 horas - Mercado de la Guindalera
<Jakeando Kañas> Evento social

05/03 - 19:00 horas - Agora de Liferay
<Los Trucos del Bugbounty>
Presenta: Jaime Andrés Restrepo

28/03 -10:00 horas - La Nave de Madrid
<Jornadas de Ingeniería Social>
Presentan: Kneda, Gema y Miguel Angel Liébanas

HACKMADRID %27

Eventos de ABRIL

07/04 - 18:30 horas - Mercado de la Guindalera
<Jakeando Kañas> Evento social

16/04 - 19:00 horas - Oficina de MNEMO
<Introducción a la Ingeniería Social>
Presenta: Kneda

18/04 -10:00 horas - La Nave de Madrid
<HackLAB: LoRaWan - Guifinet>
Presentan: David Marugan - ttnMAD - HackMadrid

HACKMADRID %27

World.Party->2020

Octubre 30/31 del 2020
Lugar: La Nave de Madrid

Una fiesta para compartir el conocimiento y el hacking inteligente

Hacking in the free world

HACKMADRID %27

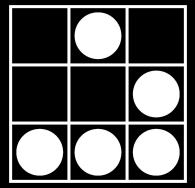
https://hackmadrid.org/flaghunters.html | Telegram: flagHunters | Telegram: t.me/hackmadrid

flagHunters CTF Team | Community

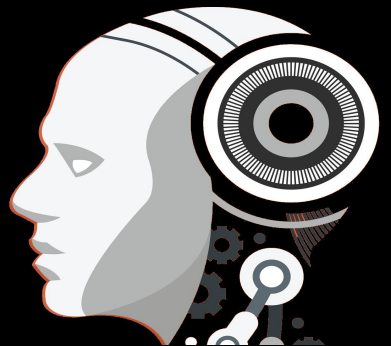
flagHunters@hackmadrid%27 ~/Documents $ cat presentacion.txt

##
HackMadrid%27 es una comunidad compuesta por miembros que desean iniciarse en la cultura "hacking" para compartir el conocimiento y hacking inteligente .:

|f|l|a|g|H|u|n|t|e|r|s| ~ es el grupo de personas de HackMadrid%27 dedicado a participar, organizar y fomentar CTF's presenciales y "online" para cualquier persona con interés en este tipo de competencias.
##



Desafío
Aptitud
Diversión
Actitud
Conocimiento
Game Over
Frustración



https://hackmadrid.org/flaghunters.html | Telegram: flagHunters | Telegram: t.me/hackmadrid

flagHunters CTF Team | Community

flagHunters@hackmadrid%27 ~/Documents $ less CTF.txt

- Capture the flag: Son juegos por Equipos o Individual, que tienen como objetivo superar diferentes retos relaccionados con habilidades de seguridad informática, consiguiendo puntos por cada prueba superada, en los cuales hay que conseguir la "Flag" (Bandera).

Flag = ctfFl4g{d6a6bc0db10694a2d90e3a69648f3a03}

Se dividen en las siguientes categorías (online o presencial):

Jeopardy: (CSAW CTF)
Reversing, Crypto, Stego, Pwn(pentest), Web, Misc(programación), Forensics, Mobile y OSINT.

Attack & Defense: (DEFCON CTF Finals)

Mixtos: Juegos de guerra, hardware, LockPicking y otros.

flagHunters CTF Team | Community

flagHunters@hackmadrid%27 ~/Documents $ less CTF.txt

¿Por qué un CTF?

- Para aprender
- Practicar habilidades
- Aprender a trabajar en equipo
- Encontrar un Empleo
- Ampliar tu círculo de amistades
- .....

Ser conscientes:

- No podemos saber de todo y va a ser frustrante y difícil
- Jugar para aprender y compartir, no para ganar
- No se para de aprender nunca, sobretodo de los errores
- Ayudar y enseñar desinteresadamente te hace ser mejor persona y mejor profesional ~ .:.

flagHunters CTF Team | Community

flagHunters@hackmadrid%27 ~/Documents $ cat plataformas_para_empezar.txt

Empezar en los CTF puede ser todo un mundo...

¡Presentamos 2 plataformas que ofrecen diversos retos + documentación sobre ellos para aprender y resolver los retos sin que te pierdas por el camino!

TRYHACKME (reto navideño + otras salas):
https://tryhackme.com/room/25daysofchristmas

ATENEA (retos básicos + Atenea Escuela):
https://atenea.ccn-cert.cni.es/escuela/home
https://atenea.ccn-cert.cni.es/challenges?category=bsica

¿Criptografía o criptología?

flagHunters@hackmadrid%27 ~/Documents/Crypto $ cat cryptography.txt

Proviene del griego kryptós que significa «oculto, secreto» y graphein cuyo significado es «escritura», o «logía», estudio.

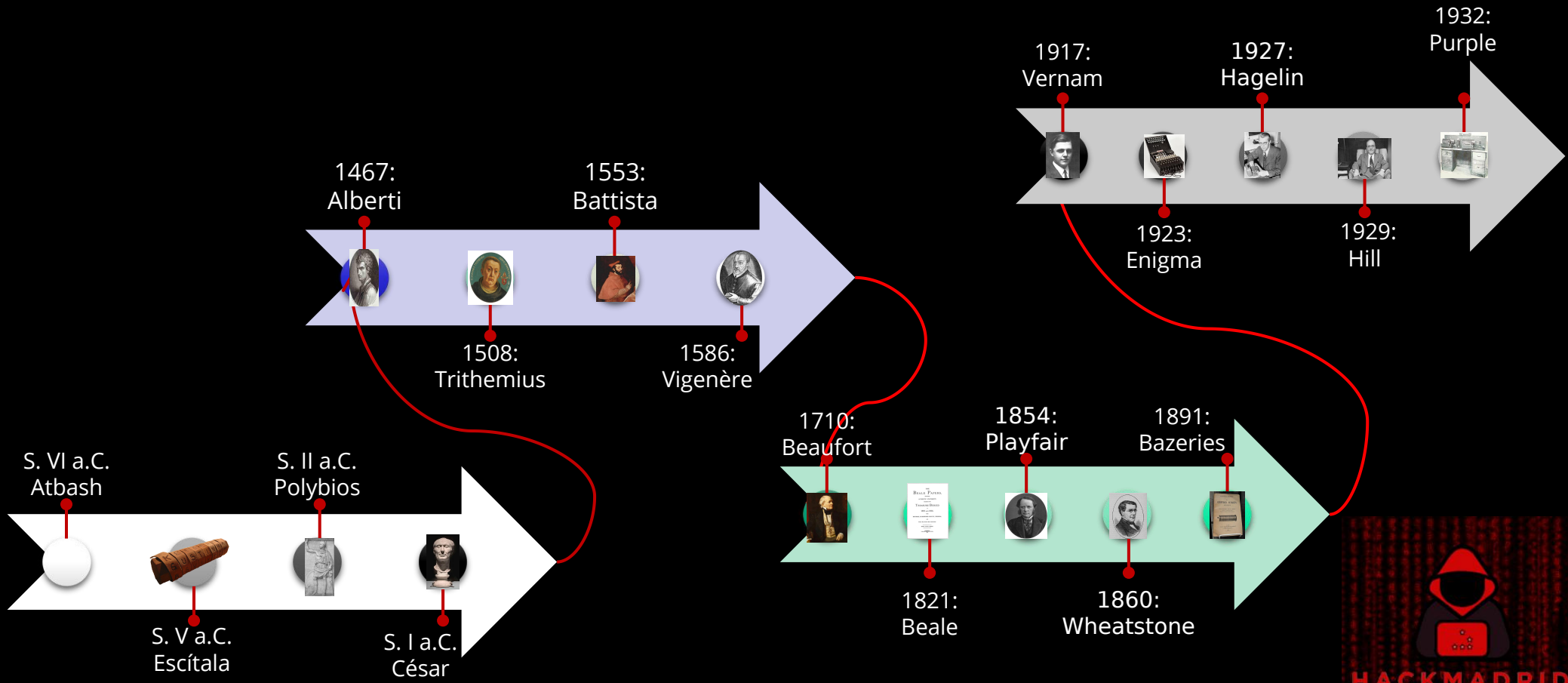
La criptología comprende 4 campos

- **Criptografía**
- **Criptoanálisis**
- **Esteganografía**
- **Estegoanálisis**
- ***¿Estegología?***

En el caso de los CTF, el objetivo suele ser descifrar o clonar objetos criptográficos o algoritmos para alcanzar la bandera.

¿Desde cuando existe la criptografía?

flagHunters@hackmadrid%27 ~/Documents/Crypto $ less cryptography_history.txt



Principios de Kerckhoffs

flagHunters@hackmadrid%27 ~/Documents/Crypto $ cat kerckhoffs.txt

1. El sistema debe ser en la práctica indescifrable, en caso de que no lo sea matemáticamente.

2. El sistema no debe ser secreto y no debe ser un problema que éste caiga en manos del enemigo.

3. La clave del sistema debe ser fácil de memorizar y comunicar a otros, sin necesidad de tener que escribirla. Será además cambiable y modificable por los interlocutores válidos.

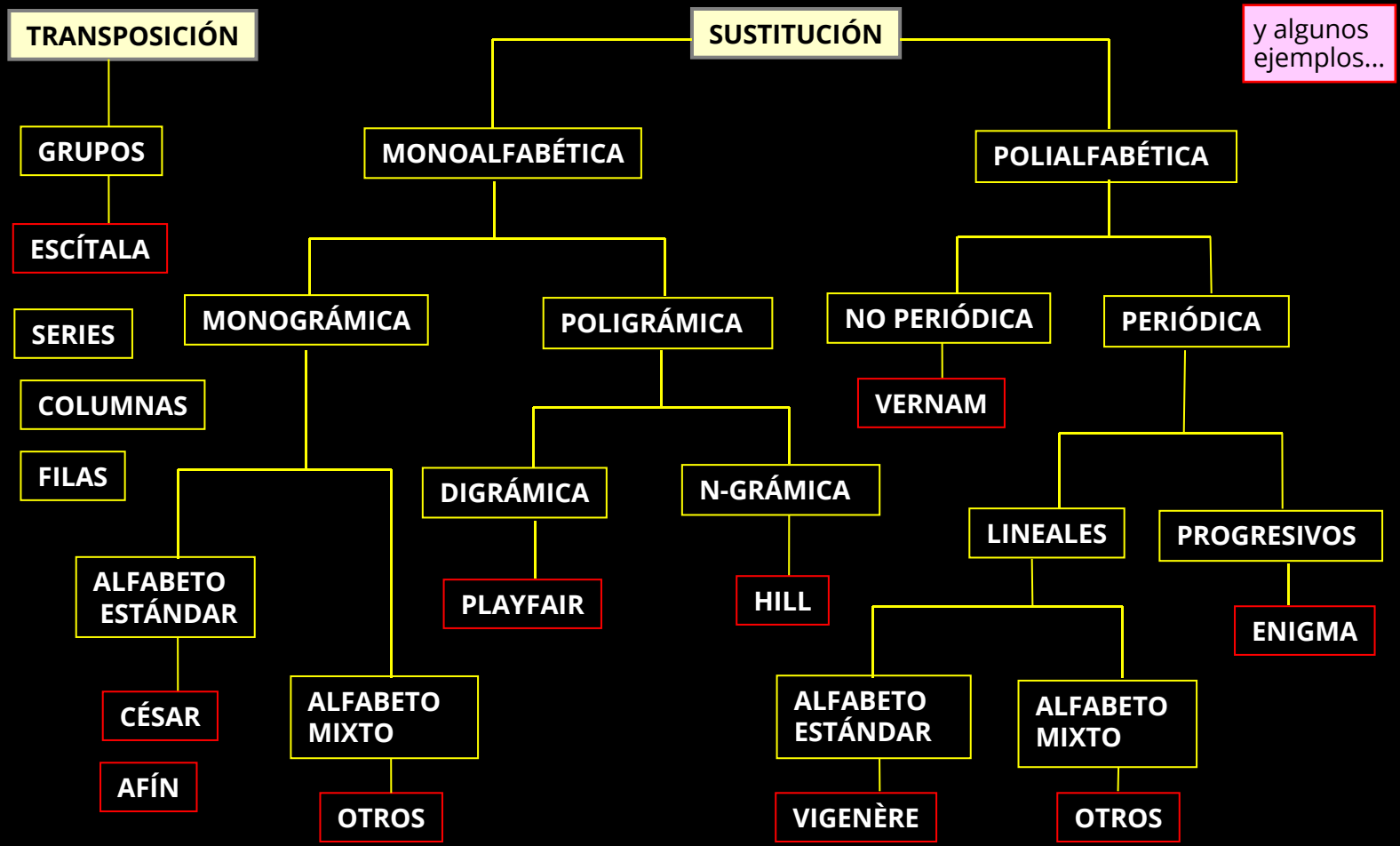
4. El sistema debe poder aplicarse a la correspondencia telegráfica.

5. El sistema debe ser portable y su uso no deberá requerir la intervención de varias personas.

6. El sistema debe ser fácil de usar, no requerirá conocimientos especiales ni tendrá una larga serie de reglas o instrucciones.

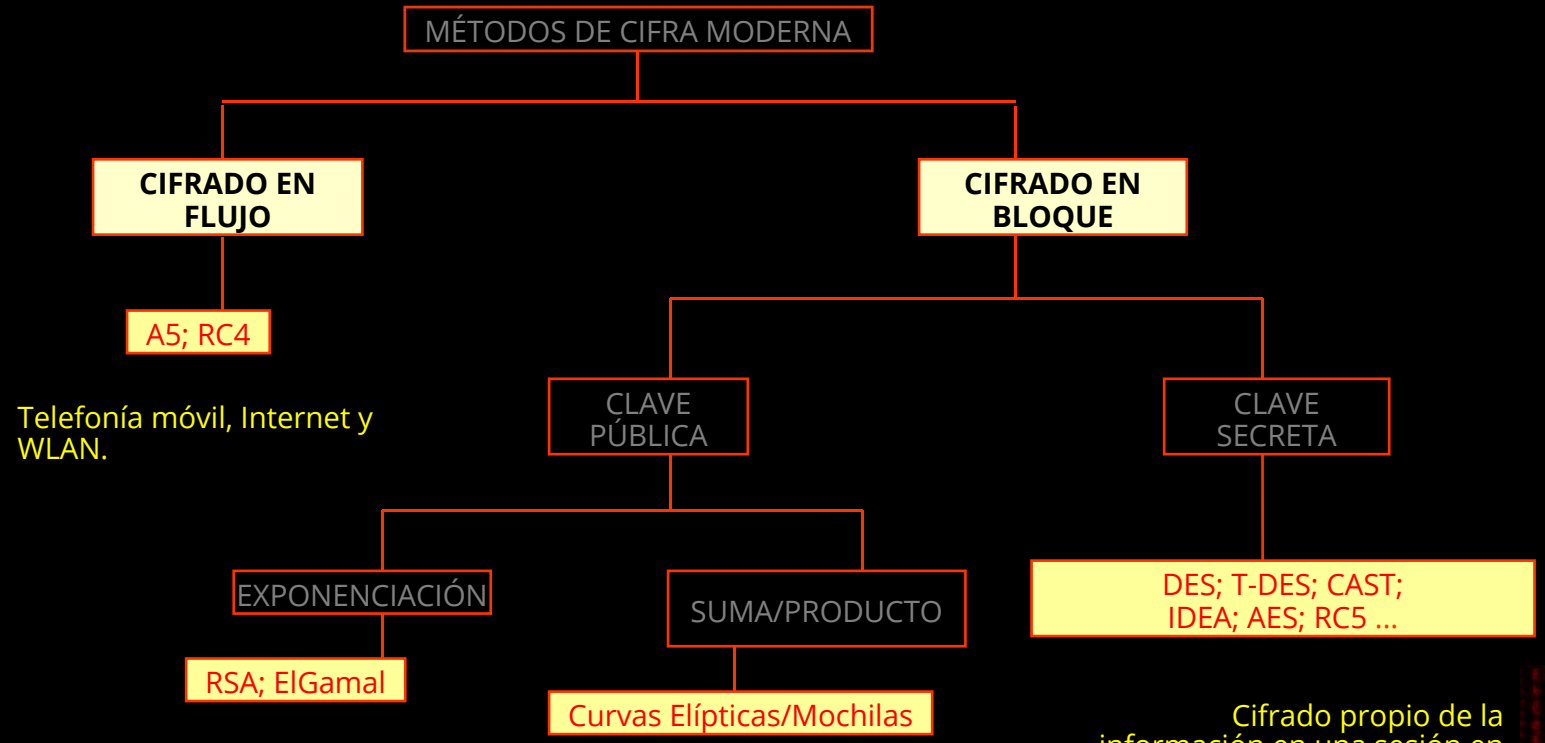
Clasificación de los criptosistemas de cifra clásica

flagHunters@hackmadrid%27 ~/Documents/Crypto $ less clasificación.txt



Clasificación de los criptosistemas de cifra moderna

flagHunters@hackmadrid%27 ~/Documents/Crypto $ less clasificación.txt



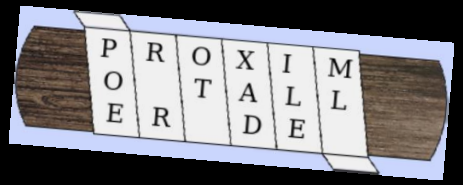
Criptografía clásica

La escítala

flagHunters@hackmadrid%27 ~/Documents/Crypto/Clásica $ cat escítala.txt

Cifrado por permutación

¿Qué herramientas necesitamos?
On-prem: **Criptoclásicos v 2.1** - http://www.criptored.upm.es/software/sw_m001c.htm
Internet: **dCode** - https://www.dcode.fr/scytale-cipher
CrypTool - https://www.cryptool.org/en/cto-ciphers/scytale
Python **CryptTools** - https://github.com/Carleslc/CryptTools



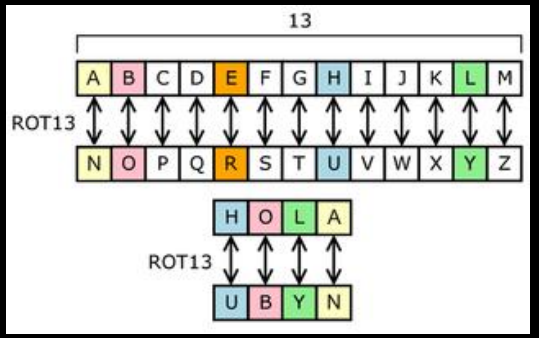
El texto en claro M es:

PROXIMOTALLERDEHACKMADRIDOSINT

El texto cifrado, o criptograma, C es:

PMLHAOROEADSOTRCRIXADKINILEMDT

El cifrador del César



flagHunters@hackmadrid%27 ~/Documents/Crypto/Clásica $ cat césar.txt

Cifrado por sustitución monoalfabético

¿Qué herramientas necesitamos?
On-prem: **Criptoclásicos v 2.1** - http://www.criptored.upm.es/software/sw_m001c.htm
Internet: **dCode** - https://www.dcode.fr/caesar-cipher
CrypTool - https://www.cryptool.org/en/cto-ciphers/caesar
Python **Hacking Secret Ciphers with Python** - https://inventwithpython.com/hackingciphers.pdf

El texto en claro M es:

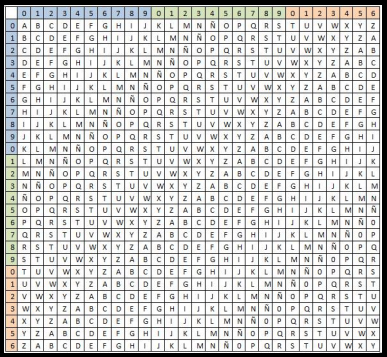
Y YA QUE HABLAS DE FREIR SI NO QUIERES QUE TE LO DEVOLVAMOS A LA ROMANA TENDRAS QUE DARNOS PRUEBAS DE TU BUENA CONDUCTA AVE

El texto cifrado, o criptograma, C es:

BBDTXHKDEÑDVGHIUHLUVLPRTXLHUHVTXHWHÑRGHYRÑYDORVDÑDURODPDWHPGUDVTXHGDUP
RVSUXHEDVGHWXEXHPDFRPGXFWDDYH

La cifra de Vigenère

flagHunters@hackmadrid%27 ~/Documents/Crypto/Clásica $ cat vigenère.txt



Cifrado polialfabético

¿Qué herramientas necesitamos?

On-prem: **Criptoclásicos v 2.1** - http://www.criptored.upm.es/software/sw_m001c.htm

Internet: **dCode** - https://www.dcode.fr/vigenere-cipher

CrypTool - https://www.cryptool.org/en/cto-ciphers/vigenere

Python **Hacking Secret Ciphers with Python** - https://inventwithpython.com/hackingciphers.pdf

Sea la clave K = BAGUETTE, y el texto en claro M es:

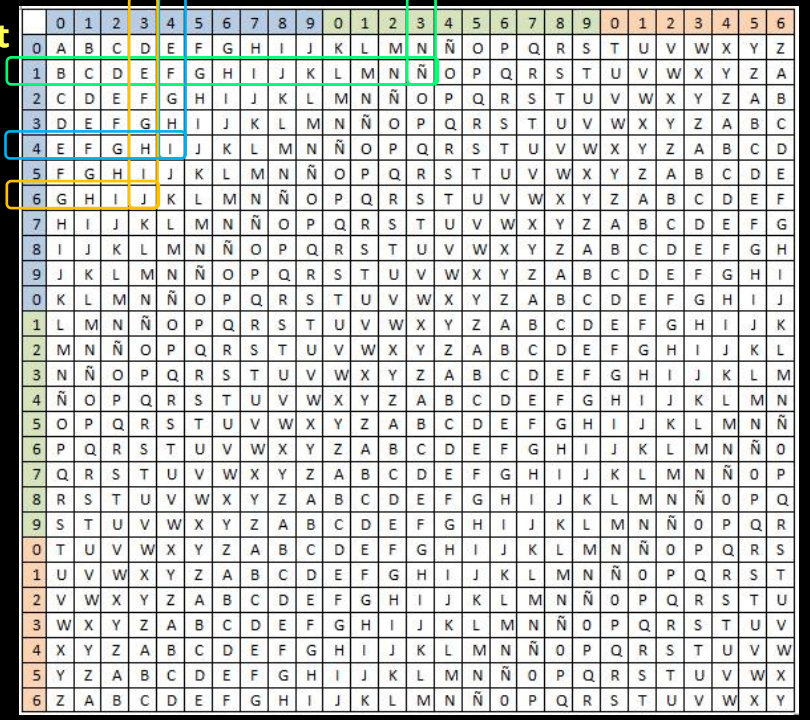
NADIESEAVERGUENZAYADECOMPORTARSEASILAHIPOCRESIAESUNAMODAYUNVICIOQUEESTADEMO
DAVIENEASERCOMOUNAVIRTUDELMEJORPAPELQUESEPUEDEDESEMPEÑARENESTOSTIEMPOSESELD
EHOMBREDEBIENYELPROFESARLAHIPOCRESIAOFRECEVENTAJASADMIRABLESESUNARTECUYAIMPOS
TURASERESPETAS IEMPREYAUNQUESEDESCUBRANADIESEATREVEACRITICARLA

El texto cifrado, o criptograma, C es:

ÑAJCIMXEWEXAYXGDBYGXIVIPQOXÑELMIBSÑFEABTPCXYWBTITUSUPIWEZUSPMVBSRUKYWNTHFMU
XEOBIÑEGNILVSNOAHEOBVUUJYOFXNPRVUTXEUVEYYTÑXHFDKNIFJIOAXYQXMXPSZCIFJSTEYYOWXLP
MHMIWXFJESSIEJVPFKNELEEIIVJGLXWJAUZVXVIWESÑECTWBDRCVTUOFSKNYGTVUEIOCTBPQOYÑYLT
WFRKNTXNETIKGTLXCBUSLYXMIEEYWYULEÑAJCIMXEURKPITVVJTÑWELEE

Vigenère - Proceso de cifrado

flagHunters@hackmadrid%27 ~/Documents/Crypto/Clásica $ cat vigenère.txt



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

Mensaje: NADIESEAVERGUENZAYADECOMPORTARSEASI

Clave: BAGUETTEBAGUETTEBAGUETTEBAGUETTE

$C_0 = (N + B) \bmod 27$
$C_0 = (13 + 1) \bmod 27 = 14 = Ñ$

$C_2 = (D + G) \bmod 27$
$C_2 = (3 + 6) \bmod 27 = 9 = J$

$C_4 = (E + E) \bmod 27$
$C_4 = (4 + 4) \bmod 27 = 8 = I$

Ataque de Kasiski


Die Geheimschriften
und
die Dechiffrir-Kunst.

Mit besonderer Berücksichtigung
der deutschen und der französischen Sprache
von
F. W. Kasiski,
Major z. D.

Berlin, 1863.
Druck und Verlag von E. S. Mittler und Sohn.

flagHunters@hackmadrid%27 ~/Documents/Crypto/Clásica $ cat vigenère_exploit.txt

Los pasos a seguir en el ataque de Kasiski son:

1. Buscar en el criptograma repeticiones de al menos 3 caracteres y anotar la distancia que separa a todas esas repeticiones.

2. Encontrar el máximo común divisor de todas esas separaciones. El mcd nos indicará la posible longitud L de la clave.

3. Se procede a dividir el criptograma en L subcriptogramas tomando las letras de L en L espacios.

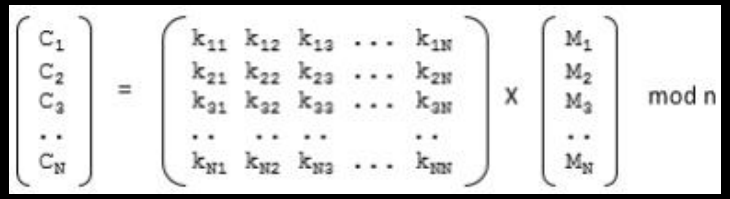
4. Para cada uno de los L subcriptogramas, se apunta la frecuencia de aparición de cada letra.

5. Se busca en cada uno de los L subcriptogramas las cuatro frecuencias más altas y que, además, cumplan con la distancia que separa a las letras con mayor frecuencia del alfabeto español mod 27, es decir la A, la E, la O y la S. Esto es, que los espacios entre ellas cumplan la siguiente distribución: Letra A -> + 4 = Letra E -> + 11 = Letra O -> + 4 = Letra S.

6. Ubicada la posición de la Letra A, que es la relativa a la letra A del texto en claro y cuyo código es igual a 0, se mira con qué letra se ha cifrado, dando así la letra correspondiente de la clave en esa posición.

7. Se repite este proceso con todos los subcriptogramas para obtener la clave buscada.

El cifrador de matrices de Hill



flagHunters@hackmadrid%27 ~/Documents/Crypto/Clásica $ cat hill.txt

Cifrado monalfabético n-grámico

¿Qué herramientas necesitamos?
On-prem: **Criptoclásicos v 2.1** - http://www.criptored.upm.es/software/sw_m001c.htm
Internet: **dCode** - https://www.dcode.fr/hill-cipher
CrypTool - https://www.cryptool.org/en/cto-ciphers/hill
Python **GitHub** - https://github.com/topics/hill-cipher?l=python

Sea la lave K = BAGUETTE, y el texto en claro M es:
MENSAJEDELESTERSANDERSHILLMATEMATICOYEDUCADORESTADOUNIDENSEQUEESTABAINTERESADOENAPLICARSUCAMPODEESTUDIOALASCOMUNICACIONESZZ

El texto cifrado, o criptograma, C es:
WZNLRJÑXEUISMIRLRNFZRPWIZNMVVEXATCVOVQDBNAJDRKTTGGOFQIFZNKQQÑZEGNACRIUNEIZSGGOYIA JVIEJRZGCXXPJGEKTTUGIDALCCCAXUXPCNNITQERYZ

Hill - Proceso de cifrado

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ .. \\ C_N \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} & \cdots & k_{1N} \\ k_{21} & k_{22} & k_{23} & \cdots & k_{2N} \\ k_{31} & k_{32} & k_{33} & \cdots & k_{3N} \\ .. & .. & .. & & .. \\ k_{N1} & k_{N2} & k_{N3} & \cdots & k_{NN} \end{pmatrix} \times \begin{pmatrix} M_1 \\ M_2 \\ M_3 \\ .. \\ M_N \end{pmatrix} \quad \text{mod n}$$

flagHunters@hackmadrid%27 ~/Documents/Crypto/Clásica $ cat hill.txt

Mensaje: MENSAJEDELESTERSANDERSHILL...

Clave:

2	20	0
18	20	0
0	0	1

Matriz inversa

5	22	0
9	14	0
0	0	1

Tabla Español 27 caracteres

Estos son los caractes ASCII incluidos dentro del **módulo 27**.

Carácter ASCII	Pos. Alfabeto	Carácter ASCII	Pos. Alfabeto	Carácter ASCII	Pos. Alfabeto	Carácter ASCII	Pos. Alfabeto
A	0	H	7	Ñ	14	U	21
B	1	I	8	O	15	V	22
C	2	J	9	P	16	W	23
D	3	K	10	Q	17	X	24
E	4	L	11	R	18	Y	25
F	5	M	12	S	19	Z	26
G	6	N	13	T	20		

Se cifrará el primer trigrama: MEN = 12, 4, 13.

C_0 = (2 * 12 (M) + 20 * 4 (E) + 0 * 13 (N)) Mod 27 = 23 (W)

C_1 = (18 * 12 (M) + 20 * 4 (E) + 0 * 13 (N)) Mod 27 = 26 (Z)

C_2 = (0 * 12 (M) + 0 * 4 (E) + 1 * 13 (N)) Mod 27 = 13 (N)

Subtexto cifrado: WZN

C = WZN LRJ ÑXE...

Ataque de Gauss-Jordan

Tabla Español 27 caracteres

Estos son los caractes ASCII incluidos dentro del **módulo 27**.

Carácter ASCII	Pos. Alfabeto	Carácter ASCII	Pos. Alfabeto	Carácter ASCII	Pos. Alfabeto	Carácter ASCII	Pos. Alfabeto
A	0	H	7	Ñ	14	U	21
B	1	I	8	O	15	V	22
C	2	J	9	P	16	W	23
D	3	K	10	Q	17	X	24
E	4	L	11	R	18	Y	25
F	5	M	12	S	19	Z	26
G	6	N	13	T	20		

flagHunters@hackmadrid%27 ~/Documents/Crypto/Clásica $ cat hill_exploit.txt

Los pasos a seguir en el ataque de Gauss-Jordan son:

Mensaje: MEN SAJ EDE...
Criptograma: WZN LRJ ÑXE...

$$\left(\begin{array}{ccc|ccc} M & E & N & W & Z & N \\ S & A & J & L & R & J \\ E & D & E & Ñ & X & E \end{array}\right) \left(\begin{array}{ccc|ccc} 12 & 4 & 13 & 23 & 26 & 13 \\ 19 & 0 & 9 & 11 & 18 & 9 \\ 4 & 3 & 4 & 14 & 24 & 4 \end{array}\right)$$

Conseguir la matriz identidad:
- Multiplicación de filas por una constante
- Restas de filas entre sí

$$\left(\begin{array}{ccc|ccc} M & E & N & W & Z & N \\ S & A & J & L & R & J \\ E & D & E & Ñ & X & E \end{array}\right) \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & K_{11} & K_{21} & K_{31} \\ 0 & 1 & 0 & K_{12} & K_{22} & K_{32} \\ 0 & 0 & 1 & K_{13} & K_{23} & K_{33} \end{array}\right)$$

$$K = \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & K_{11} & K_{12} & K_{13} \\ 0 & 1 & 0 & K_{21} & K_{22} & K_{23} \\ 0 & 0 & 1 & K_{31} & K_{32} & K_{33} \end{array}\right)$$

Conclusiones cifra clásica

flagHunters@hackmadrid%27 ~/Documents/Crypto/Clásica $ cat conclusiones.txt

- Son sistemas muy sencillos, en algún caso hasta rudimentarios, en donde resulta fácil aplicar fuerza bruta en el ataque para algunos cifrados (por ejemplo, la cifra del César).
- En algunos casos, las estadísticas y la redundancia del lenguaje nos permiten realizar ataques elegantes o criptoanálisis (por ejemplo, la cifra de Vigenère).
- En otros casos, son las matemáticas las que nos permiten criptoanalizar el sistema (por ejemplo, el cifrado de Hill con texto en claro conocido).
- Son sistemas lineales y por ello no son seguros. Algo que no ocurrirá con la criptografía moderna.

Criptografía moderna

Criptografía moderna

flagHunters@hackmadrid%27 ~/Documents/Crypto $ less cryptography_history.txt

Algoritmos simétricos

flagHunters@hackmadrid%27 ~/Documents/Crypto $ cat Simétricos.txt

BLABLABLÁ

- blablablá.

a) blablablá.
blablablá

b) blablablá.
c) blablablá.

AES

flagHunters@hackmadrid%27 ~/Documents/Crypto $ cat AES.txt

BLABLABLÁ

- blablablá.

a) blablablá.
blablablá

b) blablablá.
c) blablablá.

Criptografía asimétrica

flagHunters@hackmadrid%27 ~/Documents/Crypto $ cat Asimétricos.txt

BLABLABLÁ

- blablablá.

a) blablablá.
blablablá

b) blablablá.
c) blablablá.

RSA

flagHunters@hackmadrid%27 ~/Documents/Crypto $ cat ECDH.txt

BLABLABLÁ

- blablablá.

a) blablablá.
blablablá

b) blablablá.
c) blablablá.

Curvas elípticas

flagHunters@hackmadrid%27 ~/Documents/Crypto $ cat ECDH.txt

BLABLABLÁ

- blablablá.

a) blablablá.
blablablá

b) blablablá.
c) blablablá.

Demo Time!

Herramientas

flagHunters@hackmadrid%27 ~/Documents/Crypto $ cat Herramientas.txt

CyberChef - La navaja suiza cibernética: una aplicación web para cifrado, codificación, compresión y análisis de datos.

dCode - Sitio universal para decodificar mensajes, hacer trampa en juegos de palabras, resolver acertijos, etc.

Cryptii - Proyecto de codigo abierto en formato de aplicación web que ofrece conversión modular, codificación y cifrado en línea.

FeatherDuster - Una herramienta de criptoanálisis modular automatizada.

Hash Extender - Una herramienta útil para realizar ataques del tipo *length extension attack*.

PkCrack - Una herramienta para romper el cifrado PkZip.

RSACTFTool - Una herramienta para recuperar la clave privada RSA con varios ataques.

RSATool - Genera la clave privada conociendo p y q.

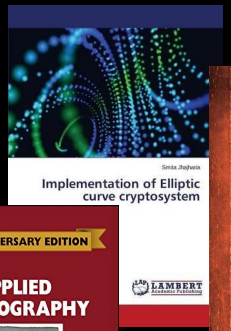
XORTool - Una herramienta para analizar cifrado xor de varios bytes.

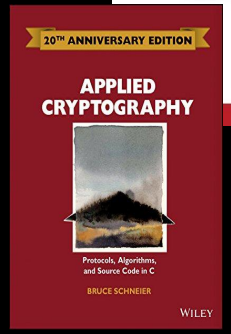
Crypto Tools For CTF - Recopilación de distintas herramientas.

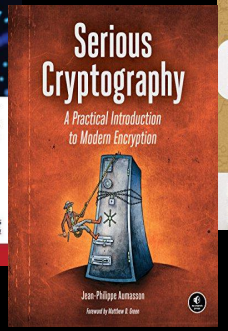
Pwntools - CTF toolkit - Pwntools es un framework para CTF y una biblioteca de desarrollo de exploits.

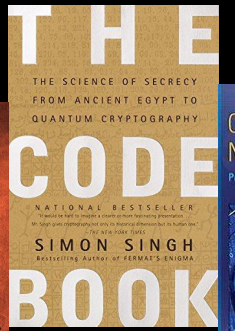
Bibliografía y recursos

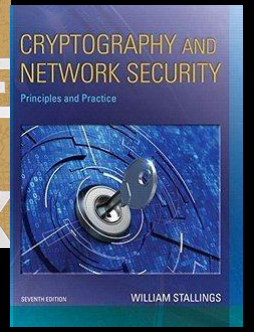
flagHunters@hackmadrid%27 ~/Documents/Crypto $ cat Bibliografía.txt







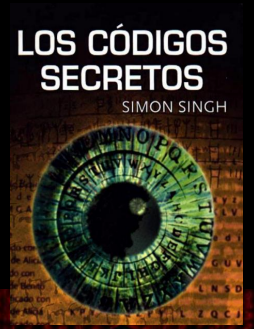




- **Libro Electrónico de Seguridad Informática y Criptografía**

Versión 4.1 de fecha 1 de marzo de 2006

- **Libro Curso de Criptografía Aplicada**
- **Proyecto MOOC Crypt4you**
- **Proyecto Cuadernos de Laboratorio de Criptografía CLCript**
- **Cifrado de las comunicaciones digitales de la cifra clásica al algoritmo RSA 2ª Edición**



- **Criptografía y Seguridad en Computadores**

Criptografía y Seguridad en Computadores: es un libro electrónico castellano, publicado bajo licencia CC.
Versión actual: 5-0.1.4 (noviembre de 2019)

SHA256 del fichero: d7349ccb415b12ca9e40f50367707aa635a9aa7a63a98562b5405c9c734be115
https://drive.google.com/open?id=1z9oVqnGqhqClfFT2-n6jR896g8-3jP_h

- **Los códigos secretos**

Un libro fascinante, original y muy ameno sobre el desciframiento de las claves y códigos secretos que han cambiado el curso de la historia, desde el Antiguo Egipto y María Estuardo, hasta las guerras mundiales y los actuales sistemas de comunicación a través del correo electrónico e Internet
http://www.librosmaravillosos.com/loscodigossecretos/pdf/Los%20codigos%20secretos%20-%20Simon%20Singh.pdf

HACKMADRID
%27

https://hackmadrid.org

https://twitter.com/hackmadrid

Telegram: t.me/hackmadrid

https://meetup.com/HackMadrid-27

https://linkedin.com/company/hackmadrid