



CRIPTOGRAFIA

Clau Simètrica



Anota en un full amb dos columnes:

En una columna:
Els que saps

En l'altra columna:
El que NO saps

PRINCIPIS DE CRIPTOGRAFIA

CRIPTOGRAFIA

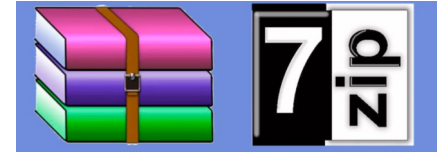
- Art o ciència de xifrar i desxifrar informació
- Del grec “**kriptos**”(ocultar) y “**graphos**”(escriure), literalment “escriptura oculta”
- S'empra per al intercanvi de missatges de manera segura, de forma que sols puguem ser llegits per les persones a les que van dirigits i que tinguen els mitjans pera desxifrar-los (**confidencialitat**)

CRIPTOLOGIA

- Com ciència engloba
 - ◆ Tècniques de xifratge: **criptografia**
 - ◆ Tècniques complementaries: el **criptoanàlisi, hashing i esteganografia**

PRINCIPIS DE CRIPTOGRAFIA

Xifrar no es comprimir



Xifrar no es codificar



Xifrar no es resumir



Xifrar no es amagar



TERMINOLOGIA DE CRIPTOGRAFIA

1. La informació original que ha de protegir-se es denomina **text en clar o text pla**
2. El **xifratge** és el procés de convertir el text pla en un text il·legible denominat **text xifrat o criptograma**
3. El **desxifrat** és el procés invers que recupera el text pla a partir del criptograma i la clau
4. **Tècniques de xifratge:**
 - **Transposició:** suposa una reordenació dels elements
 - **Substitució:** canvi de significat dels elements bàsics del missatge, les lletres, els dígit, els símbols
5. **Algorismes de xifratge** es classifiquen en:
 - De **xifratge de bloc:** divideixen el text original en blocs de bits de grandària fixa i els xifra de manera independent
 - De **xifratge de flux:** el xifratge es realitza bit a bit, byte a byte o caràcter a caràcter

EXEMPLES HISTÒRICS CRIPTOGRAFIA

L' escitalo de Esparta (siglo V a C)

Mètode de **transposició** que consistia en l'ús d'una vara de fusta (scytale) en la qual s'enrotllava una tira de cuir o papir sobre la qual s'escrivia el missatge. Quan es desenrotllava el missatge, semblava una llista sense sentit. Per a desxifrar el missatge, el destinatari simplement necessitava una vara del mateix diàmetre



Transposición de Riel

El missatge s'escriu alternant les lletres de dues línies separades. A continuació la seqüència de lletres de la línia superior, creant el missatge xifrat. El missatge es recupera simplement invertint el procés

TU SECRETO ES TU PRISIONERO; SI LO SUELTAS, TÚ ERES SU PRISIONERO
↓
T S C E O S U R S O E O I O U L A T E E S P I I N R
U E R T E T P I I N R S L S E T S U R S U R S O E O
↓
T S C E O S U R S O E O I O U L A T E E S P I I N R U E R T E T P I I N R S L S E T S U R S U R S O E O

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Escritura inversa

Mètode de **transposició** que consisteix en escriure les paraules (o frase) al revés

Transposició Columnar simple

Sense Clau TSILHKSUEYBE

Amb Clau HKSUTSILEYBE

C	A	T
2	1	3
T	H	E
S	K	Y
I	S	B
L	U	E

Transposició Per Ruta

La transposició per ruta és una tècnica de xifratge consistent a repartir el missatge a xifrar en una figura geomètrica, normalment un paral·lelepípede, encara que no és obligatori, i establir una ruta que ha de seguir-se per a llegir el missatge

Rutes: Espiral cap a dins.

Espiral des del centre

Manera diagonal

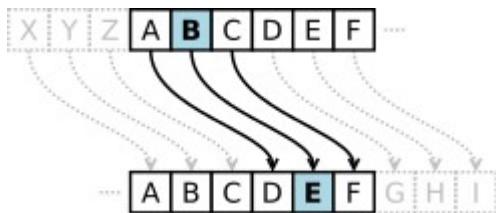
Per columnes

E	U	F
O	R	I
C	A	S

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifrat César

Sistema de **substitució** que consisteix a reemplaçar cada lletra del text per una altra que es troba un nombre de posicions més endavant en l'alfabet



Julio César solia utilitzar un desplaçament de 3 posicions en quasi tots els seus missatges

Texto original: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Texto codificado: DEFGHIJKLMNOPQRSTUVWXYZABC

ROT13 (rotar 13 posicions)

ABECEDARIO ORIGINAL

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cifrado CESAR - Despl. +13

MNOPQRSTUVWXYZABCDEFGHIJKL

ABECEDARIO CIFRADO



EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifrat César

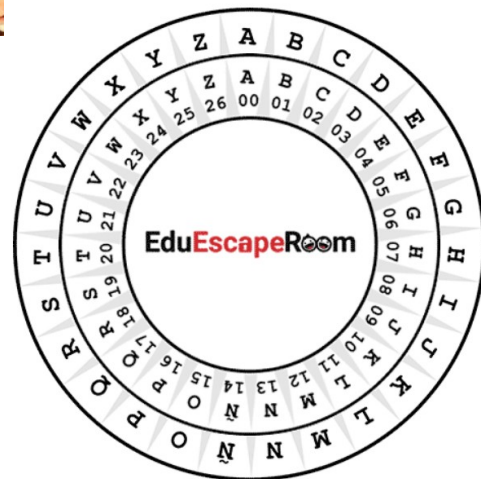
Utilitza la pàgina <https://es.planetcalc.com/1434/>

Per desxifrar el següent missatge

Ix zofnqmdoxcfx bp jmiq afsboqfax. cixd: CkxdFsnoxdPobbob

¿Falta alguna cosa?

¿Que es pot observar en el missatge xifrat?



SCRIPT XIFRAT

Exemple d'algorisme de substitució: comando tr

Per Xifrar mitjantsant codificació César un archiu de text pla:

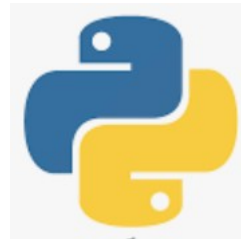
```
cat archivo | tr [a-z] [d-zabc] | tr [A-Z] [D-ZABC]> doc.cesar
```

El comando **tr** permet realitzar una substitució caràcter a caràcter mitjançant canonades (pipes) s'ha incorporat majúscules i case límit com són els caràcters 'x', 'y', 'z'

Pràctica

- 1) Crea un fitxer en text pla
- 2) Xifra el fitxer amb el comando anterior
- 3) Verifica el contingut del fitxer
- 4) Desxifra el fitxer i comprova que el resultat és el mateix que l'original

ALGORISME DE XIFRAT I DESXIFRAT



Exemple d'algorisme de substitució: algorisme en python

Per Xifrar mitjantsant codificació César un missatge

Proposa
algorisme !

Pràctica

- 1) Crea dos fitxers amb els algorismes `xifra.py` i `desxifra.py`
- 2) Xifra una cadena
- 3) Desxifra la cadena

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge Vigenère

És un xifratge basat en diferents sèries de caràcters o lletres del xifratge César formant aquests caràcters una taula, anomenada taula de Vigenère. El xifratge de Vigenère és un xifratge per substitució simple polialfabètic.

Es pot utilitzar una clau per a anar agafant cíclicament les sèries

<https://es.planetcalc.com/2468/>

ATACARALANOCHECER
LIMONLIMONLIMONLI
lbmqncixoazktsppz

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge Vigenère

<https://es.planetcalc.com/2468/>

Missatge: pdkjavw a yjksnxmfj, otl zx ujrwiçfj

Clau: (inicials d'un institut meravellos a Algemesí)

¿Que es pot observar en el missatge xifrat?

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge Ottendorf

També anomenat Xifratge per Llibre, consisteix en una sèrie de grups de tres números que fan referència a lletres específiques en un llibre.

Aquest llibre ha de ser conegut pel descodificador, i ser a més de la mateixa edició que el llibre de la persona que escriu el missatge codificat.

Dels grups de números, el primer (començant per l'esquerra) correspon a la pàgina del llibre.
El segon a la línia i el tercer a la lletra.

Per exemple: Triem el llibre "La volta al món en 80 dies",
volem escriure de forma xifrada "JULES VERNE". Una possibilitat seria aquesta:

39-6-30
53-1-2
65-3-7
18-12-4
162-19-1
223-2-14
88-22-10
183-4-5
9-8-3
144-5-9

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge A1Z26

És un xifratge per substitució directa molt simple, on cada lletra de l'alfabet es reemplaça pel seu número en l'alfabet.

A continuació, es mostra el codificador/descodificador A1Z26. Aquest és un xifratge per substitució directa molt simple, on cada lletra de l'alfabet es reemplaça pel seu número en l'alfabet.

Ací totes les lletres es posen en minúscules, s'usa l'alfabet anglés i no es transformen tots els símbols que no pertanyen a l'alfabet. En la descodificació, tots els números (de l'1 al 26) han d'estar separats per qualsevol símbol que no siga un dígit (guió, espai, etc.)

Variants: A1Z27 (poden incloure la ñ) o A0Z26

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge Atbash

És un mètode de codificació de l'alfabet hebreu que consisteix a utilitzar la lletra simètrica a la donada segons el següent esquema:

Cifrado Atbash

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

També se'l coneix com a mètode d'**espill**

A=Z | N=M

B=Y | O=L

C=X | P=K

D=W | Q=J

E=V | R=I

F=U | S=H

G=T | T=G

H=S | U=F

I=R | V=E

J=Q | W=D

K=P | X=C

L=O | Y=B

M=N | Z=A

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge de Polibi

És un mètode de codificació de l'alfabet grec.
Pot codificar 25 símbols. (5x5)



https://es.wikipedia.org/wiki/Cuadrado_de_Polibio

<https://museo.inf.upv.es/blog/2021/05/14/cifrado-de-polibio/>

MENSAJE ORIGINAL

MUI XE R A N G A

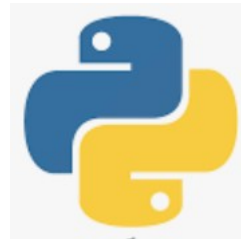
CRIPTOGRAMA

3 3 5 1 2 4 5 4 1 5 4 3 1 1 3 4 2 2 1 1

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

Es pot ampliar a 36 amb una matriu de 6x6

ALGORISME DE XIFRAT I DESXIFRAT



Exemple d'algorisme de substitució: algorisme en python

Per Xifrar mitjantsant codificació de Polibi un missatge

Proposa
algorisme !

Pràctica

- 1) Crea dos fitxers amb els algorismes `xifrapol.py` i `desxifrapol.py`
- 2) Xifra una cadena
- 3) Desxifra la cadena

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge Vernam

És un xifratge de flux en el qual el text en clar es combina, mitjançant l'operació **XOR**, amb un flux de dades aleatori o pseudoaleatori de la mateixa grandària (clau), per a generar un text xifrat. L'ús de dades pseudoaleatòries generades per un generador de números pseudoaleatoris criptogràficament segur és una manera comuna i efectiva de construir un xifratge en flux.

El RC4 és un exemple de xifratge de Vernam que s'utilitza amb freqüència en **Internet**.

T	E	X	T	O	84	69	88	84	79	1010100	1000101	1011000	1010100	1001111
C	L	A	V	E	67	76	65	86	69	1000011	1001100	1000001	1010110	1000101
XOR					23	9	25	2	10	10111				
hex					17	9	19	2	A					

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge Vernam

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

Missatge: 23 0d 0d 44 05 0b 02 4a 41 27 10 10 04 42 1b 0d 07 10 02 10 41 07 10 44 0c 07 10 44 02 0d 0e
14 0d 0b 00 05 15 4c

Clau: abcd

EXEMPLES HISTÒRICS CRIPTOGRAFIA

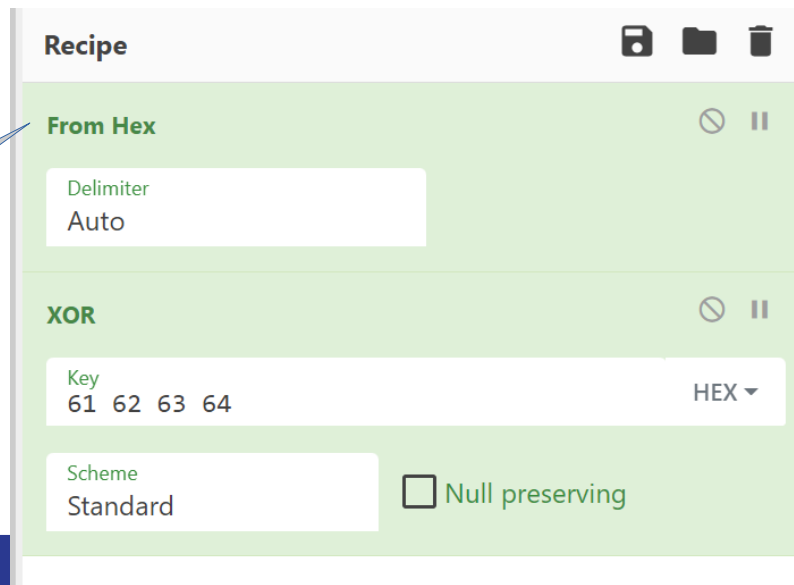
Xifratge Vernam

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

Missatge: 23 0d 0d 44 05 0b 02 4a 41 27 10 10 04 42 1b 0d 07 10 02 10 41 07 10 44 0c 07 10 44 02 0d 0e
14 0d 0b 00 05 15 4c

Clau: abcd 61 62 63 64

Com XOR actua a nivell
de bit, hem de convertir
primer en bits



The image shows a screenshot of the CyberChef web application interface. The 'Recipe' panel is active, displaying a list of recipes. The 'XOR' recipe is selected and expanded, showing its configuration. The 'From Hex' section is visible, with a 'Delimiter' dropdown set to 'Auto'. The 'XOR' section shows a 'Key' input field containing the hexadecimal values '61 62 63 64', with a 'HEX' dropdown menu to its right. The 'Scheme' dropdown is set to 'Standard'. There is an unchecked checkbox for 'Null preserving'.

Recipe

From Hex

Delimiter
Auto

XOR

Key
61 62 63 64 HEX ▾

Scheme
Standard ☐ Null preserving

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge Enigma

Era el nom d'una màquina de rotors que permetia usar-la tant per a xifrar com per a desxifrar missatges. La seua facilitat de maneig i suposada inviolabilitat van ser les principals raons per al seu ampli ús.

La màquina Enigma va ser un dispositiu electromecànic, cosa que significa que usava una combinació de parts mecàniques i elèctriques. El mecanisme estava constituït fonamentalment per un teclat similar al de les màquines d'escriure les tecles de les quals eren interruptors elèctrics, un engranatge mecànic i un panell de llums amb les lletres de l'alfabet.

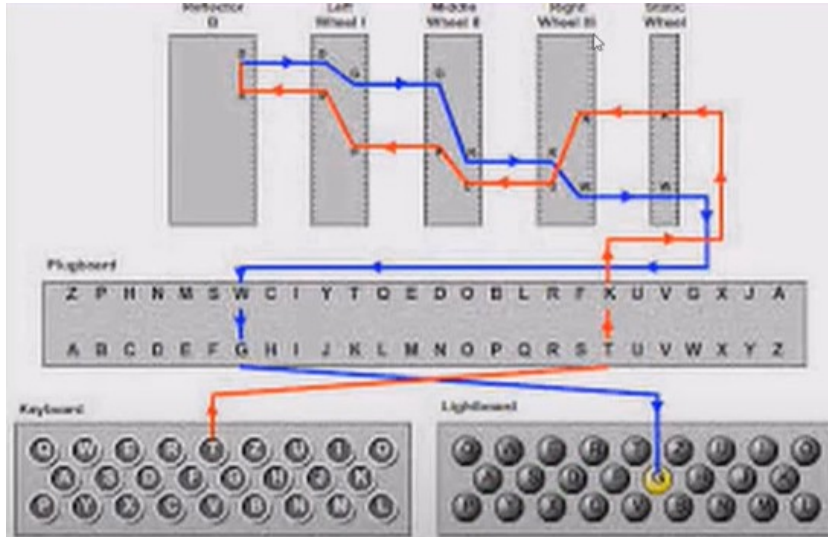
<https://summersidemakerspace.ca/projects/enigma-machine/>

Les claus que es subministren: Model, Deflector, Rotors, Anells, Claviller



EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge Enigma : Funcionament



EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge Enigma :

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

Missatge: VBCUH QMCDY HSCJX YJFON QILXB WOWYR E

Clau:

Rotor esquerre S

Rotor central V

Rotor dret F

Recipe

Enigma

Model
3-rotor

Left-hand rotor
EKMFLGDQVZNTOWY...

Left-hand rotor ring s...
S

Left-hand rotor init...
A

Middle rotor
AJDKSIRUXBLHWTM...

Middle rotor ring s...
V

Middle rotor initial...
A

Right-hand rotor
BDFHJLCPRTXVZNY...

Right-hand rotor ri...
F

Right-hand rotor initial value
A

Reflector
AY BR CU DH EQ FS GL IP J...

Plugboard

☒ Strict output

EXEMPLES HISTÒRICS CRIPTOGRAFIA

Xifratge per codificació

¡¡ Els algorismes de codificació (e.g. Base64) **no són algorismes de xifratge**, es descodifiquen fàcilment i, per tant, no ha d'utilitzar-se com un mètode de xifratge segur. No utilitzeu aquesta tècnica per a protegir les dades confidencials, per la qual cosa ha d'utilitzar mètodes de xifratge segurs !!

No obstant això, cal considerar el format d'una informació xifrada amb la condició d'analitzar per on es començarà a descodificar / desxifrar.

Formats habituals.

ASCII

HEXADECIMAL

BASE64

BINARIO

SCRIPT XIFRAT

Algunes web de xifratge

<https://es.planetcalc.com/1434/>

<https://www.convertstring.com/ca/EncodeDecode/Base64Encode>

<https://www.rapidtables.com/convert/number/hex-to-ascii.html>

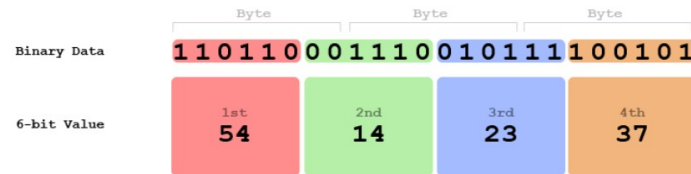
<https://gchq.github.io/CyberChef/>

<https://cryptii.com/>

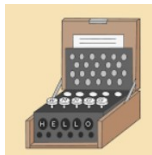
<https://www.dcode.fr/>



Base64 Encoding



{UTF-8}



TIPUS D'ALGORISMES DE XIFRATGE

(2º) Principi de Kerckhoffs (La Cryptographie Militaire) 1883

En seguretat i criptografia, principi segons el qual la seguretat d'un sistema xifrat ha de dependre exclusivament de la clau i no de la seguretat de qualsevol una altra part del sistema.

S'ha de suposar, així, que el sistema pot caure en mans del “enemic” i que pot analitzar-la tant com vulga, però que la falta de la clau li impedirà entendre el codi xifrat.

Així, els algorismes són públics i es poden estudiar i valorar per tal d'escollir el que més s'ajuste a les nostres necessitats.

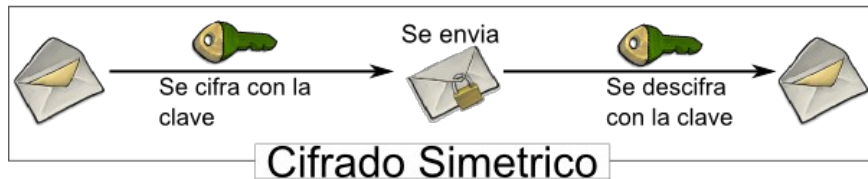
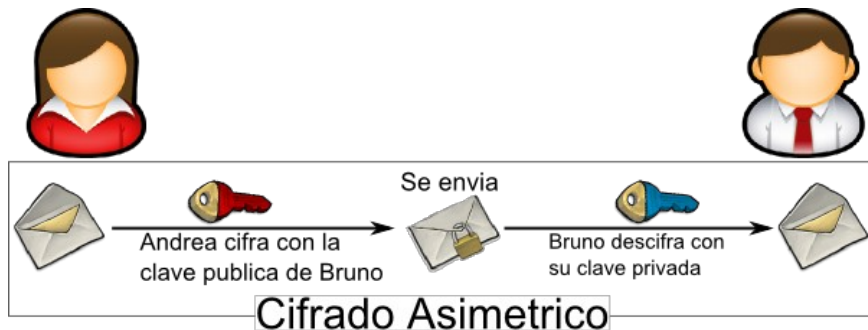


CRIPTOGRAFIA MODERNA

TIPUS D'ALGORISMES DE XIFRATGE

Existeixen dos grans tipus d'algorismes de xifratge:

- ➔ **Simètrics o de clau simètrica** : usa una única clau tant en el procés de xifratge com en el desxifrat
- ➔ **Asimètrics o de clau asimètrica o pública**: usen una clau per a xifrar missatges i una clau diferent per a desxifrar-los. Formen el nucli de les tècniques de xifratge modernes (certificat digital, signatura digital, DNle)



CRIPTOGRAFIA SIMÈTRICA

- S'usa una **mateixa clau per a xifrar i desxifrar** missatges
- Les dues parts que es comunica han d'acordar per endavant sobre la clau a usar
- Un bon sistema de xifratge posa tota la seguretat en la clau i cap en l'algorisme:
 - ◆ La clau ha de ser molt difícil d'endevinar
 - ◆ **Important: longitud de la clau i conjunt de caràcters que empre**



CRIPTOGRAFIA SIMÈTRICA

Exemples d'algorismes de xifratge simètric:

- ➔ **DES** (Data Encryption Standard IBM 1975) triat estàndard FIPS: usa una clau de 56 bits => hi ha 2^{56} claus possibles (72.057.594.037.927.936). Utilitza xifratge de Feistel. Successor d'algorisme Lucifer
- ➔ **3DES**, (IBM 1998) usa claus de 128 bits el que significa que existeixen 2^{128} claus possibles (targetes de crèdit) (340.282.366.920.938.463.463.374.607.431.768.211.456)

En 1997, l'Institut Nacional de Normes i Tecnologia (NIST) va decidir realitzar un concurs per a triar un nou algorisme de xifratge capaç de protegir informació sensible durant el segle XXI. Aquest concurs es va denominar Advanced Encryption Standard (AES).

RIJNDAEL: 86 vots

SERPENT: 59 vots

TWOFISH: 31 vots

RC6: 23 vots

MARS: 13 vots

CRIPTOGRAFIA SIMÈTRICA

Exemples d'algorisme de xifratge simètric:

- ➔ **DES** (Data Encryption Standard any 1976): usa blocs de 64 i una clau de 64 bits (56 bits). Utilitza la funció F de **Feistel**
- ➔ **IDEA** (International Data Encryption Algorithm 1991) usa blocs de 64 bits i clau de 128 bits. (No F)
- ➔ **Blowfish** (1993) usa blocs de 64 bits i claus que van des dels 32 bits fins a 448 bits (16 rondes F)
- ➔ **3DES** (IBM 1998) triple-des. usa blocs de 64 i una clau de 168 bits (112 bits). Utilitza F de Feistel
- ➔ **AES** (Advanced Encryption Standard 2001) o Rijndael (**Raindoll**) (estàndard de xifratge usat pel govern dels Estats Units). Usa una grandària de bloc fix de 128 bits i clau de 128, 192 o 256 bits
- ➔ **RC6** (Rivest Cypher 6) usa grandària de bloc de 128 bits i accepta claus de grandària 128, 192 i 256
- ➔ **Serpent** usa una grandària de bloc de 128 bits i suporta grandàries de clau de 128, 192 i 256 bits
- ➔ **Mars** (Presentat per IBM) blocs de dades de 128 bits i claus de longitud variable de 128 a 448 b
- ➔ **Kuznyechik** Xifratge per blocs simètric. El qual té una grandària de bloc de 128 bits i una longitud de clau de 256 bits. Està definit en l'Estàndard Nacional de la Federació Russa
- ➔ **Camellia** (Japó) amb una grandària de bloc de 128 bits i grandàries de clau de 128, 192 i 256 bits

CRIPTOGRAFIA SIMÈTRICA

AES (Advanced Encryption Standard) o **Rijndael** (Raindoll) (estàndard de xifratge usat pel govern dels Estats Units). Usa una grandària de bloc fix de 128 bits i clau de 128, 192 o 256 bits)

Missatge: 2259206c3308406be9d0ae30d610bf32bc0c2a417a346bf3c3c3be620575db96

Clau : 1234567890abcdef

IV: abcdef0987654321

Utilitza CyberChef

Contesta:

De quina grandària és la clau ?

Fixat en el missatge i en la clau. En quina codificació estan cadascú ?

CRIPTOGRAFIA SIMÈTRICA

Els principals problemes dels sistemes de xifratge simètric:

→ L'intercanvi de claus

- ◆ Quin canal de comunicació segur han usat per a transmetre's les claus?
- ◆ Més fàcil per a l'atacant intentar interceptar una clau que provar totes les possibles combinacions.

→ El nombre de claus que es necessiten

- ◆ Per a n persones que necessiten comunicar-se entre si, es necessiten $n(n-1)/2$ claus diferents
- ◆ 90 persones -> 4.005 claus 300 persones -> 44.850 claus 6000 persones -> 17.997.000 claus
- ◆ Funciona amb un grup reduït de persones

→ Fortalesa de la clau

- ◆ **Principi de Kerckhoffs** i
- ◆ La responsabilitat de la fortalesa de la clau recau sobre l'usuari

CRIPTOGRAFIA SIMÈTRICA

XIFRAT DE DADES. ccrypt en Linux

- ➔ Eina per a xifrar i ocultar en l'ordinador dades que l'usuari consideri reservats o confidencials
- ➔ Utilitza : Rijndael/256 (el mateix que **AES**)
- ➔ Sobreescriu els sectors originals (ho intenta)

```
sudo apt-get install ccrypt
ccrypt archivo // Encripta el archivo
ccrypt -d archivo // Desencripta el archivo

ccrypt -R carpeta // Encripta la carpeta
ccrypt -dR carpeta // Desencripta la carpeta
```

```
(kali@kali)-[~]
$ cccrypt archivo
Command 'ccrypt' not found, but can be installed with:
sudo apt install cccrypt
Do you want to install it? (N/y)
```

Tutorial cccrypt
Usage cccrypt 

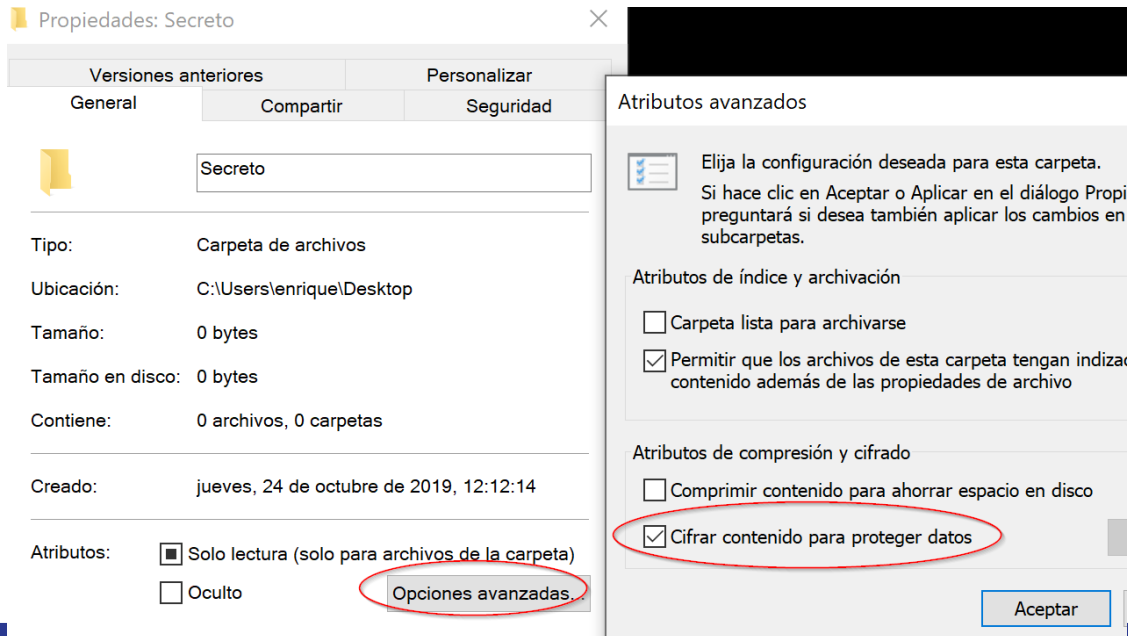
Pràctica

Encriptar un arxiu i una carpeta amb cccrypt utilitzant una clau simètrica. Observar els resultats.

CRIPTOGRAFIA SIMÈTRICA

XIFRAT DE DADES. Sistema EFS de Windows

- ➔ Eina per a protegir la sortida de dades del sistema
- ➔ Utilitza :**AES + SHA + ECC**



Pràctica

Encriptar una carpeta amb Windows EFS. Copiar-la a un ordinador d'un company i observar si es pot accedir.

¿On està la clau?

CRIPTOGRAFIA SIMÈTRICA

XIFRAT DE DADES I PARTICIONS

VeraCrypt

- ➔ Eina per a xifrar i ocultar en l'ordinador dades que l'usuari considere reservats o confidencials
- ➔ Ofereix la possibilitat de crear discos virtuals o aprofitar una partició ja existent per a desar fitxers xifrats
- ➔ Permet triar entre diversos algorismes de xifratge: **AES, Camellia, Kuznyechik, Serpent, Twofish**

<https://www.veracrypt.fr/en/Downloads.html>

Práctiques

- 1) Crear un disc encriptat en windows
- 2) Protegir un pendrive amb contasenya

CRIPTOGRAFIA SIMÈTRICA

Pràctica

Muntar un volum encriptat des de la consola de linux

1. Instal·lar veracrypt

Des de la pàgina de downloads, baixa la versió adequada

<https://www.veracrypt.fr/en/Downloads.html>

Obri-la amb l'instal·lador de Ubuntu

2. Encriptar un fitxer com un volum virtual

CRIPTOGRAFIA SIMÈTRICA

Pràctica

Muntar una carpeta per xifrar dades en us

En linux / kali

1. Instal·lar la utilitat **cryFS** (visita la pàgina oficial www.cryfs.org)

Preparar dos carpetes basedir i mountdir

Muntar encriptació `cryfs basedir mountdir`

Guardar, modificar dades dins de mountdir (mai en basedir !!)

Observar (sols observar) basedir

2. **Desmuntar encriptació**

`cryfs-unmount mountdir` (o reiniciar, o eixir de sessió d'usuari)

FUNCIONS HASH

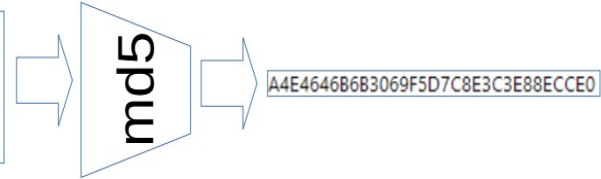
Funcions resum o funcions hash (també funcions digest)

- Els sistemes asimètrics es recolzen en **funcions resum** o **funcions hash** d'un sol sentit. El seu càlcul directe és viable, però la funció inversa resulta quasi impossible (**computacionalment intractable**)
- El resum sempre té una **longitud fixa** i xicoteta (típicament 128 o 256 bits)
- Xicotets canvis en el document produeixen grans canvis en el hash
- Algorismes emprats com a funcions resum o funcions hash: exemples: **MD5 i SHA**

Las funciones hash no son reversibles



Las funciones hash no son reversibles, a partir del resultado o huella digital no se puede obtener el texto de origen.



Las funciones hash no son reversibles, a partir del resultado o huella hash no se puede obtener el texto de origen.



FUNCIONS HASH

→ Usos

- ◆ Analitzar la integritat d'un arxiu (iso, programa,...) verificar la seua autenticitat
- ◆ Magatzematge de contrasenyes d'usuari, arxiu /etc/shadow de GNU/Linux
- ◆ Signatura digital d'arxius, mail, etc
- ◆ Detectar malware
- ◆ Protecció de contingut protegit (copyright)
- ◆ Tecnologies Blockchain i SmartContracts



FUNCIONS HASH

Exemple d'ús de funcions resum

- ➔ Analitzar la integritat d'un arxiu descarregat mitjançant la comprovació del seu valor resum calculat
- ➔ En moltes ocasions, les web dels fabricants originals mostren al costat del seu arxiu d'instal·lació del valor resumeixen calculat, amb el qual podrem verificar després de descarregar l'arxiu d'instal·lació la seua integritat o que no ha sigut modificat o és una falsificació

Exemple pràctic windows

- ➔ Descarrega una iso de la pàgina <http://ophcrack.sourceforge.net/download.php>
- ➔ Descarrega la utilitat md5 de la pàgina <http://www.fourmilab.ch/md5/>
- ➔ Comprova si s'ha descarregat correctament (la iso)

Ejemplo GNU/Linux / KALI

- ➔ Executem `md5sum archivo.txt > archivo.md5`
- ➔ Verifiquem la integritat del arxiu: `md5sum -c archivo.md5`

FUNCIONS HASH



MD5

- ➔ La funció hash MD5 produeix un valor hash de 128 bits (16 Bytes o 32 nibbles). Va ser dissenyat per al seu ús en criptografia, però es van descobrir vulnerabilitats amb el pas del temps, per la qual cosa ja no es recomana per a aqueix propòsit. No obstant això, encara s'utilitza per a particionar bases de dades i calcular sumes de comprovació per a validar les transferències d'arxiu

SHA1

- ➔ SHA1 genera un hash de 160 bits (20 bytes o 40 nibbles). En format hexadecimal, és un nombre enter de 40 dígits. Igual que MD5, va ser dissenyat per a aplicacions de criptologia, però prompte es va descobrir que també tenia vulnerabilitats. Hui dia, ja no es considera menys resistent a l'atac que MD5

SHA2

- ➔ La segona versió de SHA, anomenada SHA-2, té moltes variants. Probablement el més utilitzat és SHA-256, que el NIST recomana usar en lloc de MD5 o SHA-1. L'algorisme SHA-256 retorna un valor hash de 256 bits o 64 dígits hexadecimals

SHA3 Aquest mètode hash es va desenvolupar a la fi de 2015 i encara no ha tingut un ús generalitzat

FUNCIONS HASH

Pràctica

Utilitza les funcions

`md5sum`

`sha1sum`

`sha224sum`

`sha256sum`

`sha384sum`

`sha512sum`

de linux per a calcular resums d'arxius i observa els resultats. Utilitza l'opció `-c` per a comprovar la integritat de l'arxiu original

FUNCIONS HASH

SHA3 No té suport en linux com a ordre directa, però podem utilitzar la suite Openssl

```
$ openssl help
```

Message Digest commands (see the `dgst' command for more details)

blake2b512	blake2s256	gost	md4
md5	mdc2	rmd160	sha1
sha224	sha256	sha3-224	sha3-256
sha3-384	sha3-512	sha384	sha512
sha512-224	sha512-256	shake128	shake256
sm3			

```
$ openssl dgst -sha3-256 texto.plano
```

```
(kali@kali)-[~]  
$ openssl dgst -sha3-256 archivo  
SHA3-256(archivo)= ad015c3dff3cb222649c24e3c68acc7e46d67a81df70368ccc1305dff8b8ae8a
```

FUNCIONS HASH

Com es trenca un Hash

- Força bruta (Eina John , HashCat, Hash Suite - <https://hashsuite.openwall.net/>)
- Force bruta amb diccionaris
- Rainbow Tables (<https://crackstation.net/> o similars)
- Atacant l'algorisme específic



FUNCIONS HASH

Altres funcions HASH

WHIRLPOOL

Streebog

CRC

Tiger

Snefru

RipeMD

MD2 MD4

Haval

Adler

Gost

....

.... <https://hash.online-convert.com/>

Funcions HASH Lentes (especials per a passwords)

- Argon2
- scrypt
- bcrypt
- PBKDF2

FUNCIONS HASH

Pràctica

Busca informació sobre la història de TrueCrypt

Qui va ser el seu creador

Perquè la seua desaparició

Qui ha heretat les seues funcionalitats



TrueCrypt

FUNCIONS HASH

Pràctica

Calcula HASHes en Windows

Instal·la i utilitza el programa per a calcular hashes

<https://www.quickhash-gui.org/downloads/>



Visita la pàgina oficial, i contesta....

- Per a quins Sistemes Operatius està disponible ?
- Quins algorismes de hash pot calcular ?
- Quines altres ferramentes oferix la web ?

FUNCIONS HASH

Pràctica

Calcula HASHes en Windows

PowerShell



Busca informació de com visualitzar un hash en PowerShell

Calcula el hash d'un arxiu amb els tipus de hash:

md5, sha1, sha256, sha512, sha384

Calcula el hash d'una cadena "Hola Mon"

I visualitza TOT els hash complets !!

Contesta: **Si no se especifica un tipus de hash, quin hash calcula per defecte ??**