



Práctica 1: Introducción a la Criptografía: Seguridad de Sistemas Informáticos

Cheuk Kelly Ng Pante
alu0101364544@ull.edu.es
Nicolás Joaquín Miranda Lizondo
alu0101683027@ull.edu.es



1. Seleccionar 3 Dorks	2
2. Cifrado de texto con cifrado César	5
3. Expresión matemática asociada al Cifrado de César	5
4. Descifrado de los siguientes criptogramas	6
5. ¿Es el cifrado de César un cifrado monoalfabético?	7
6. Descifrar los siguientes criptogramas con el cifrado multiplicativo.	7
7. Cifrado de Vigenere	8
8. Descifrado de Vigenere	9
9. ¿Cuál es la expresión matemática que define el cifrado de Vigenere?	9
10. Cifrar usando Playfair	10
11. Descifrar usando Playfair	10
12. Máquina enigma. Compara la descripción dada allí con la ofrecida en la web de Cryptool Online.	11



1. Seleccionar 3 Dorks

- `intitle: "Index of ftp passwords"`

El operador `intitle` se utiliza para buscar páginas webs cuyos títulos contienen una palabra o frase específica. El parámetro `"Index of ftp passwords"` se refiere a una frase clave que estamos buscando en los títulos de las páginas. La frase sugiere que estamos interesados en encontrar páginas que puedan contener listas de contraseñas de FTP.



Bernadette Rottler

<https://48fep.bernadetterottler.de>

Intitle index of ftp password

hace 2 días — `inc intitle:"index of" intext:globals. txt 2022-12-17 20:05 311K all_id. Intitle: "Index of ftp passwords" - Files Containing trend www. 4 ...`



autopetri.de

<https://48fep.autopetri.de>

Intitle index of ftp password

hace 3 días — `Listing intitle:index. Intitle: "Index of ftp passwords" - Files Containing trend www. 3M : 1id-index. pub. 00 seconds (53000 For *nix, most ...`



world4family.de

<https://vpujnubpr.world4family.de>

Intitle index of ftp password

hace 2 días — `... intitle:admin intitle:loginLeapFTP intitle:"index. Feb 12, 2002 · Securing ... Index of ftp passwords" Google Search: intitle: "Index of ftp ...`



svm-srb.de

<https://vpujnubpr.svm-srb.de>

Intitle index of ftp password

`etc" passwd intitle:admin intitle:loginLeapFTP intitle:"index.. of etc shadow ... Index of ftp passwords" # Files Containing Passwords # Date:12/09/2021 ...`



Imagine Digit

<https://fmddkapur.imagedigit.de>

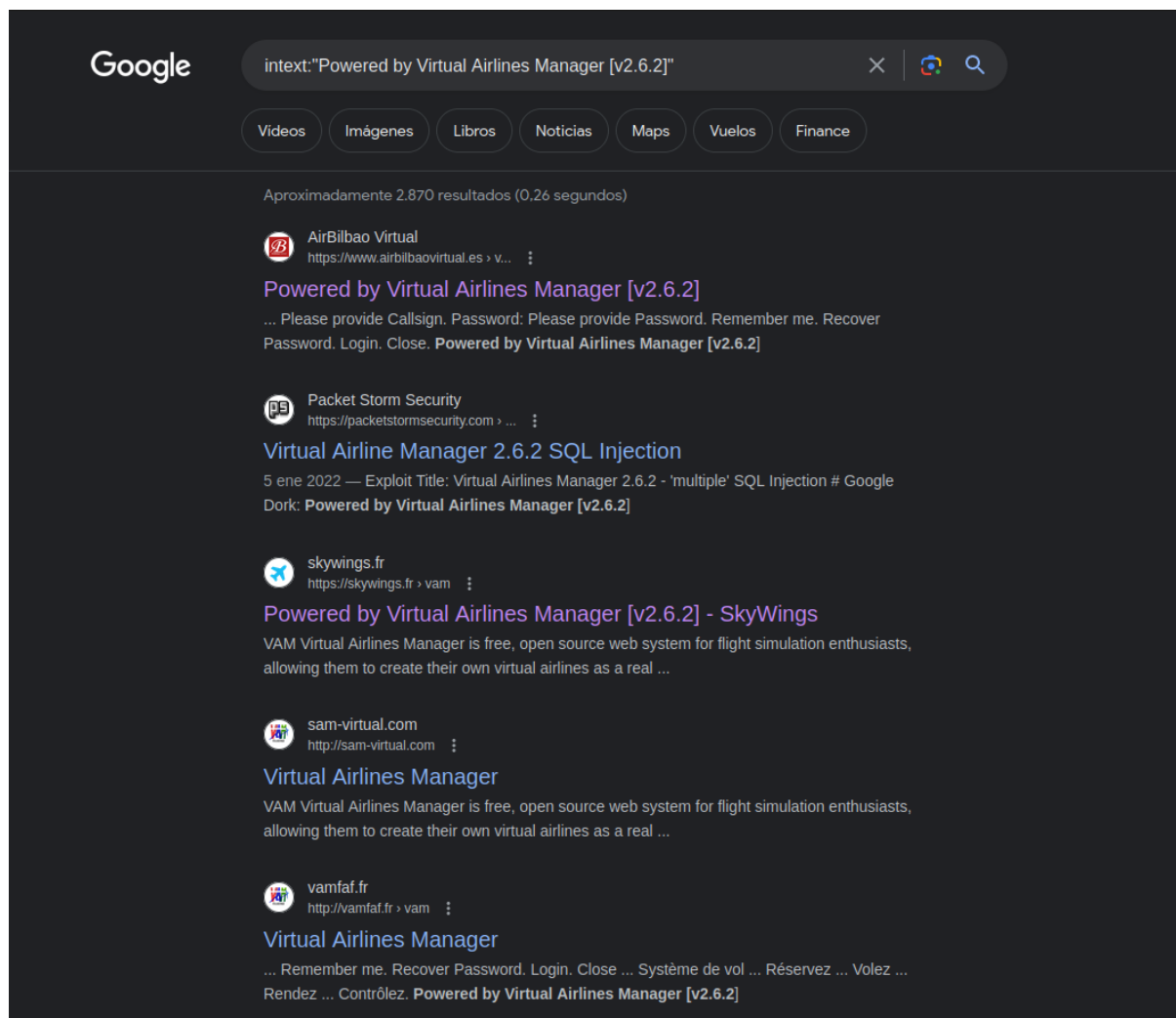
Intitle index of ftp password

`... intitle: "Index of ftp passwords" Google Search: intitle: "Index of ftp passwords" # Google Dork: intitle: "Index of ftp passwords" # Files Containing ...`



- `intext:"Powered by Virtual Airlines Manager [v2.6.2]"`

Busca en las páginas en las cuales está el texto exacto “Powered by Virtual Airlines Manager [v2.6.2]”, busca aquellos sitios web los cuales tienen la versión especificada de Virtual Airlines Manager.





- `intitle:Index of "/venv"`

Encuentra resultados de los motores de búsqueda en los cuales están de manera pública y que tienen una carpeta llamada “venv”. Nos podría dar directorios en servidores web los cuales tienen archivos o recursos relacionados con Python.

intitle:Index of "/venv"

Imágenes Videos Noticias Libros Maps Vuelos Finance

Aproximadamente 9.840 resultados (0,33 segundos)

Sugerencia: Limita esta búsqueda a resultados en **español**. Más información sobre cómo filtrar por idioma

52.50.135
<http://52.50.135.160> > venv

Index of /venv

Index of /venv. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -, [DIR], bin/, 2022-03-21 22:27, -, [DIR], include/, 2022-03- ...

itcollege.ee
<https://enos.itcollege.ee> > ~adroz d

Index of /~adroz d/skriptimiskeeled/venv

Index of /~adroz d/skriptimiskeeled/venv. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -, [DIR], bin/, 2019-04-23 13:54, -, [...

3.126.181
<http://3.126.181.200> > venv

Index of /venv

Index of /venv. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -, [DIR], bin/, 2021-12-27 21:57, -, [DIR], include/, 2021-12- ...

Brookhaven National Laboratory (.gov)
<https://www.phy.bnl.gov> > ~yuhw

Index of /~yuhw/larsoft855/src/wct/python/venv

Index of /~yuhw/larsoft855/src/wct/python/venv. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -, [DIR], bin/, 2021-03-11 01: ...

totalfoods.in
<https://totalfoods.in> > venv

Index of /venv - Total Foods

Index of /venv. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory,



2. Cifrado de texto con cifrado César

Cipher

Description

Input (plaintext)

length: 396

Holmes had been seated for some hours in silence with his long, thin back curved over a chemical vessel in which he was brewing a particularly malodorous product. His head was sunk upon his breast, and he looked from my point of view like a strange, lank bird, with dull gray plumage and a black top-knot. "So, Watson," said he, suddenly, "you do not propose to invest in South African securities"

Encrypt Decrypt

Key: - 1 +

Output (ciphertext)

length: 396

Ipmnft ibe cffo tfbufe gps tpnf ipvst jo tjmfodf xjui ijt mpoh, uijo cddl dvswfe pwfs b difnjdbm wfttfm jo xijdi if xbt csfxjoh b qbsujdvmszmz nbmpepspvt qspevdu. Ijt ifbe xbt tvol vqpo ijt csfbtu, boe if mpplfe gspn nz qpjou pg wjfx mjlf b tusboh, mbol cjse, xjui evmm hsbz qmvsbhf boe b cmbdl upq-lop. "Tp, Xbutpo," tbje if, tveefomz, "zpv ep opu qspqptf up jowftu jo Tpvui Bgsjdbo tfdvsjujft"

Input (plaintext)

length: 397

"Holmes had been seated for some hours in silence with his long, thin back curved over a chemical vessel in which he was brewing a particularly malodorous product. His head was sunk upon his breast, and he looked from my point of view like a strange, lank bird, with dull gray plumage and a black top-knot. "So, Watson," said he, suddenly,"you do not propose to invest in South African securities"

Encrypt Decrypt

Key: - 5 +

Output (ciphertext)

length: 397

"Mtqrjx mfi gjjs xjfyji ktw xtrj mtzwx ns xqjshj Bnym mnx qtsl, ymns gfhp hzwAji tAjw f hmjrnfhq Ajxxjq ns Bmnhm mj Bfx gwjBnsl f ufwynhzqfwqD rfqtitwtzx uwtizhy. Mnx mjfi Bfx xzsp zuts mnx gwjfy, fsi mj qttppi kwtr rD utnsy tk AnjB qnpj f xywfslj, qfsp gnwi, Bnym izqq lwfD uqzrflj fsi f gqfhp ytu-psty. "Xt, bfyxts," xfni mj, xziijsqD,"Dtz it sty uwtutxj yt nsAjxy ns Xtzym Fkwnhfs xjhzwnynjx"

3. Expresión matemática asociada al Cifrado de César

- Cifrado: $C(x) = (x + k) \bmod n$
- Descifrado: $D(x) = (x - k) \bmod n$
 - $C(x)$ es la letra cifrada y $D(x)$ es la letra descifrada.
 - x es la letra original.
 - k es el desplazamiento.
 - n es el tamaño del alfabeto.



4. Descifrado de los siguientes criptogramas

- PBZ CHG REF PNA ORN CNV AVA GUR OEN VA:

Cipher

Description

Input (plaintext) length: 38

PBZ CHG REF PNA ORN CNV AVA GUR OEN VA

Encrypt ☐ Decrypt

Key:

-

 13

+

Output (ciphertext) length: 38

cOm PUT eRS caN bea Pai NiN The bRa iN

- GZZG IQOT ZNKK BKTO TMUX GZJG CT:

Cipher

Description

Input (plaintext) length: 32

GZZG IQOT ZNKK BKTO TMUX GZJG CT

Encrypt ☐ Decrypt

Key:

-

 20

+

Output (ciphertext) length: 32

atta ckin thee Veni ngor atda Wn

- WKHHP SHURU KDVEH HQDVV DVVLQ DWHG

Cipher

Description

Input (ciphertext) length: 33

WKH HPSHURU KDV EHHQ DVVDVVLQDWHG|

Encrypt ☒ Decrypt

Key:

-

 3

+

Output (plaintext) length: 33

THE EMPEROR HAS BEEN ASSASSINATED



5. ¿Es el cifrado de César un cifrado monoalfabético?

Sí, el cifrado de César es un tipo de cifrado monoalfabético. Cada letra del alfabeto se reemplaza por otra. En el cifrado de César se realiza un desplazamiento fijo a lo largo del alfabeto, dependiendo del tipo de desplazamiento fijado.

6. Descifrar los siguientes criptogramas con el cifrado multiplicativo.

- qtFyKycK yc FVm PayFV FVaF hmaJc FQ agVymLmKmnF:

OPTIMISM IS THE FAITH THAT LEADS TO ACHIEVEMENT

Encrypted text:

qtFyKycK yc FVm PayFV FVaF hmaJc FQ agVymLmKmnF

- NQFVyns gan Dm JQnm oyFVQiF VQtm anJ gQnPyJmngm:

NOTHING CAN BE DONE WITHOUT HOPE AND CONFIDENCE


Encrypted text:

NQFVyns gan Dm JQnm oyFVQiF VQtm anJ gQnPyJmngm

Ambas se encuentran en un factor de multiplicación por 3.



7. Cifrado de Vigenere



Vigenère

First strong polyalphabetic cipher

Cipher

Description

Background

Security

About alphabets

Plaintext:

DESASTRE NUCLEAR EN MURUROA

↓

Encrypted text:

VSKSGLJS FMQDW0J WB EMFMJCS

Key:

SOS



8. Descifrado de Vigenere

Plaintext:

MARI PURI APAGA ESE ORDENADOR

↑

Encrypted text:

IIEI DOJE ICDUW WOM BURAFWLBU

Key:

WINDOWS

9. ¿Cuál es la expresión matemática que define el cifrado de Vigenere?

Sería la siguiente expresión:

$$C_i = (M_i + K_i) \% 26$$

Ci es la letra cifrada

Mi es el número/posición que representa la letra en el mensaje

Ki es el número/posición que representa la letra en la clave

Y el % 26 nos aseguramos que el resultado esté entre el rango de letras del alfabeto



10. Cifrar usando Playfair

Square size: ☒ 5x5 ☐ 6x6

Enter plaintext to be enciphered:

LA SOMBRA DEL VIENTO

Enter keyword: DANIEL SEMPERE

Select keyword route: Rows from top left

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

☐ 5-letter groups ☒ 2-letter groups ☐ No punctuation or spaces

Cipher:

SD CW LF SE AD BD ED IQ QW

11. Descifrar usando Playfair

Square size: ☒ 5x5 ☐ 6x6

Enter plaintext to be enciphered:

FP LV MT SO RH LB VN

Enter keyword: EVANESCENCE

Select keyword route: Rows from top right

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

☐ 5-letter groups ☐ 2-letter groups ☒ No punctuation or spaces

Cipher:

BRINTZETOLIFEA



12. Máquina enigma. Compara la descripción dada allí con la ofrecida en la web de Cryptool Online.

Cryptool Online se centra en la configuración y funcionamiento específico de la máquina Enigma, detallando aspectos técnicos como las ruedas con desbordamiento, compensación, la creación de permutaciones personalizadas y el desplazamiento de las letras en las ruedas. En resumen, proporciona información detallada sobre cómo se pueden configurar y utilizar las ruedas en una máquina Enigma para cifrar y descifrar mensajes.

Por otro lado, el video se centra en aspectos más generales y conceptuales sobre la máquina Enigma. Se mencionan aspectos como la importancia de elegir los rotores correctos, la configuración de los rotores en términos de opciones disponibles y posiciones de inicio, y la tabla de conexiones que añadía dificultad a la configuración. Este enfoque se centra en comprender la importancia de la elección de rotores y la configuración general de la máquina, pero no entra en detalles técnicos específicos como lo hace Cryptool Online.