

Seguridad

Tema: Práctica 1 - Criptografía en la práctica



Participantes

Carlos Javier Hellín Asensio (carlos.hellin@edu.uah.es)

Darius Dumitras Tamas (darius.tamas@edu.uah.es)

Grado de Ingeniería Informática

Curso: 2021-2022

Cifrado César	3
Cifrado Vigenere	5
One-time Pad	6


Cifrado César

1. Acceda a esta [web](#).

a) Cifre y descifre varias frases cambiando el nº de posiciones a desplazar

Mensaje 1:

mensaje original:

Codificador / Descodificador de cifrado César	
 Prueba también el Transformador de palabras en emojis 🍷🍷🍷	
Texto:	
	<u>Hello</u> World
Número de posiciones a desplazar: 3	
Codificar	Descodificar

Mensaje 1 cifrado con clave 3.

Codificador / Descodificador de cifrado César	
 Prueba también el Transformador de palabras en emojis 🍷🍷🍷	
Texto:	
	<u>Khoor</u> <u>Zruog</u>
Número de posiciones a desplazar: 3	
Codificar	Descodificar

Mensaje 2:


Codificador / Descodificador de cifrado César	
 Prueba también el Transformador de palabras en emojis 🍷🍷🍷	
Texto:	
	<u>Alistate en la marina</u>
Número de posiciones a desplazar: 8	
Codificar	Descodificar

Mensaje 2 cifrado con clave 8:

Codificador / Descodificador de cifrado César	
 Prueba también el Transformador de palabras en emojis 🍷🍷🍷	
Texto:	
	<u>Itaqiblm</u> <u>mv</u> <u>ti</u> <u>uizqvi</u>
Número de posiciones a desplazar: 8	
Codificar	Descodificar

b) ¿Por qué a este número de posiciones se le llama clave en este cifrado?
Debido a que si se cambia este número de posiciones, se obtienen mensajes codificados diferentes.

2. Cifre el siguiente mensaje: “En un lugar de la mancha de cuyo nombre no quiero acordarme” con una clave de desplazamiento de 3.

Codificador / Descodificador de cifrado César	
 Prueba también el Transformador de palabras en emojis 🥰🥳🌈	
Texto:	
En un lugar de la mancha de cuyo nombre no quiero acordarme	
Número de posiciones a desplazar: 3	
Codificar	Descodificar

Codificador / Descodificador de cifrado César	
 Prueba también el Transformador de palabras en emojis 🥰🥳🌈	
Texto:	
<u>Hq xq oxidu gh od pdafkd gh fxbr qrpeuh qr txlhur dfrugduph</u>	
Número de posiciones a desplazar: 3	
Codificar	Descodificar

3. Reflexione sobre las siguientes cuestiones:

a) ¿Depende el cifrado del diccionario usado? ¿Por qué?

- Si, porque si existiese un diferente número de caracteres en el diccionario, la letra a la cual se le corresponderá el mensaje final cambiaría. Por ejemplo, no es lo mismo codificar A con desplazamiento 3 en un diccionario “AÄÄBCÇ”, el cual daría un mensaje final de B, mientras que si trabajamos con un diccionario “ABCDE” obtendremos el mensaje final de “D”.

b) ¿Qué sucede con los espacios en blanco del texto a cifrar?

- Los espacios en blanco se mantienen con la codificación.

c) ¿Cree que es fácilmente descifrable? ¿Repetición de secuencias cifradas?

- Es un algoritmo de cifrado en el que es factible descifrar un mensaje por el método de fuerza bruta, además, el conocimiento del diccionario facilita la descifración.

- Por mucho que se codifique el mensaje múltiples veces, no se cifra de forma diferente a como se cerraría un mensaje con clave $n \cdot \text{clave_actual}$.

Cifrado Vigenere

a) Utilizando el cifrado de Vigenère y la clave: **aurora**, explique el procedimiento seguido y descifre el siguiente mensaje:

“Eh lb cugui rv la grbtha xv qlyo hfasre hf elielv otorxrfde”

teniendo como clave:

“au ro raaur or aa uroraa ur oraa uroraa ur oraaaur oraaaurora”

	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

El primer paso es, mirando la primera fila, siendo su índice la primera letra de la clave, parándose en el carácter de mensaje y, subiendo a la columna, obtenemos el carácter correspondiente al mensaje original.

El mensaje final es:

En un lugar de la Mancha de cuyo nombre no quiero acordarme

One-time Pad

Acceda a este [enlace](#):

- Genere distintos mensajes cifrados con distintas claves, y apúntelas.
- Proceda a descifrarlos.

Mensaje 1

Encrypt ▾

Your message:

Rico es un buen nombre

The pad:

laaalssslldaisdidsd

Cico pk mf mxew frvejh

Mensaje 1 descifrado

Decrypt ▾

Your message:

Cico pk mf mxew frvejh

The pad:

laaalssslldaisdidsd

Rico es un buen nombre

Mensaje 2

Encrypt ▾

Your message:

Rafael Lopez son buenos apellidos

The pad:

euuwiikfasbxhdashidhiqweieew

Vuvvmu Vtpwa pvq bmlwrz jfapurhso

Mensaje 2 descifrado.

Decrypt ▾

Your message:

Vuvvmu Vtpwa pvq bmlwrz ifapurbso

The pad:

euqwiikfasbxdashidhiqweiiww

Rafael Lopez son buenos apellidos

• Reflexione sobre los siguientes aspectos:

1. ¿Tamaño de la clave/frente al texto?

- Cuanto mayor sea el tamaño de la clave, más grande tendrá que ser el texto, y viceversa, debido a que la clave tiene que ser del mismo tamaño que el texto. También, cuanto más pequeño sea el texto más seguro será, debido a que existirán menos patrones a seguir.

2. ¿Es posible siempre garantizar una clave distinta?

- No, debido a que las claves en mensajes muy cortos (más seguros) acabarían terminándose, por ejemplo, en las claves asociadas a un mensaje de longitud 1, es mucho más fácil de ver que el número de claves es finito.

c) Cifre la siguiente secuencia 0110 1101 1111 0101 con un algoritmo One-Time Pad utilizando la clave

1110 0101 0001 1111

obteniendo el resultado en binario y en hexadecimal.

0110 1101 1111 0101

1110 0101 0001 1111

1000 1000 1110 1010

8 8 E A

d) Explique el procedimiento que ha seguido.

El procedimiento que se ha seguido es la realización de la puerta lógica xor entre la secuencia y la clave.

Criptografía Simétrica

Ahora van a cifrar un fichero cualquiera para garantizar su confidencialidad, utilizando una clave privada a través de un sencillo servicio web (<https://vmola.com/file-encryption.php>)

clave inicial: lacontrasenamaslargaquesemeocurre

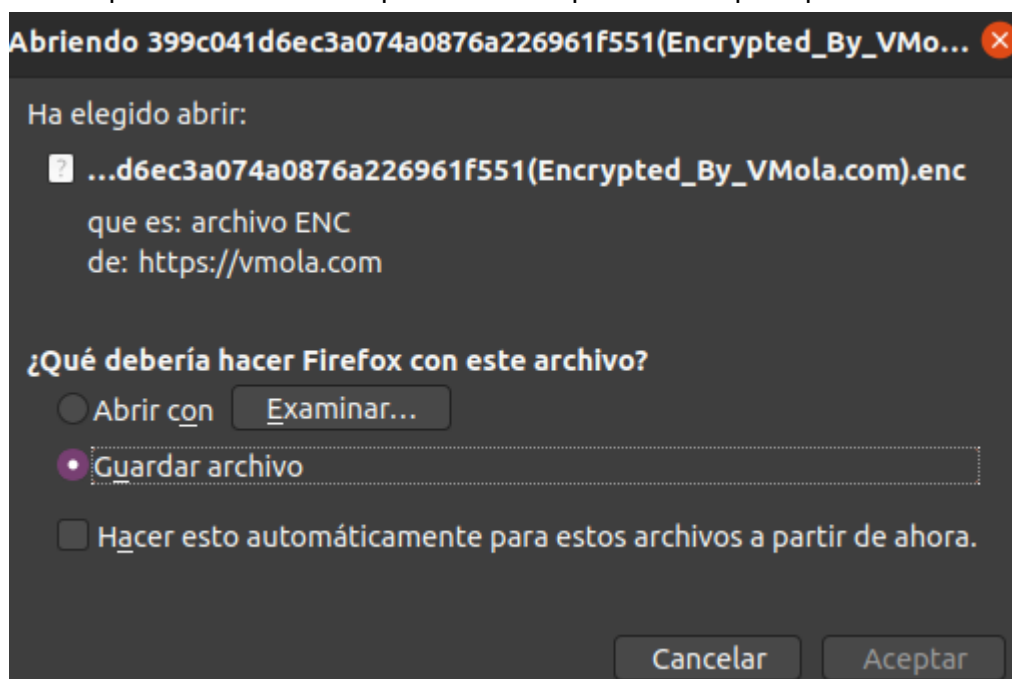
segunda clave: eltamañonoimporta

I - Pruebe con una clave de distinto tamaño de la inicial: ¿Cambia el tamaño del fichero cifrado?

El tamaño del archivo es el mismo independientemente de la contraseña.

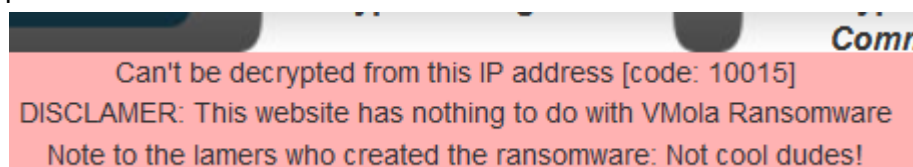
II - Investigue el funcionamiento de las 3 opciones que se muestran (Change Filename, Hide file's extensión & Lock this file...)

La primera opción: change filename cambiará el nombre del fichero, la segunda opción cambiará la extensión a .enc y la tercera opción hará que no se pueda descryptar desde otra IP que no sea desde la que se ha encriptado en un principio.



III - Compruebe el bloqueo de un archivo cifrado asociado a una dirección IP:

1. Puede cifrar otro fichero usando esta opción y comprobando con sus compañeros/as del puesto a su derecha si funciona correctamente.



2. Indique qué funcionalidades se le ocurren a este bloqueo por IP en conjunto con el cifrado.

Restringir aún más el acceso al fichero cifrado, siempre que la IP pública se mantenga fija.

c) Ahora pruebe a cifrar otro fichero con un clave_1 y el resultado lo vuelve a cifrar con una clave_2. Compruebe con sus compañeros/as si se puede recuperar el fichero original.

clave1: laclave1

clave2: laclave2

A partir del archivo doblemente cifrado se ha podido recuperar primero el archivo cifrado 1 vez y después el archivo original, además, el tamaño de los archivos ha variado entre encriptaciones, la segunda encriptación aumentó el tamaño del archivo.

2.1. Criptografía Simétrica 6 3.

Ahora van a generar un entorno de mensajería seguro utilizando el cifrado simétrico.

Siguiendo en este servicio web (<https://8gwifi.org/CipherFunctions.jsp>):

a) Tiene que conseguir enviar un mensaje a sus compañeros/as del puesto a su derecha, confidencial utilizando cualquiera de los algoritmos que aparecen. Puede enviar el mensaje cifrado por e-mail o WhatsApp.

b) ¿Cómo ha compartido la clave?

Se ha subido un txt por drive con la clave a descifrar, al igual que con los mensajes 1 y 2 cifrados.

c) Cifre a su vez la clave con otro algoritmo antes de pasársela a sus compañeros/as y repita el proceso.

Primera desenscriptación:

Cipher

AES/ECB/PKCS5PADDING

eHCa1pTENP53fSIW9xWuxtPd6Mzry17E/1JYy2eycXo=

SecretKey

2b7e151628aed2a6abf71589

☐ Encrypt

☒ Decrypt

Submit

resultado de la primera descifración, obtenemos como resultado la clave.

[decrypt]

[eHCa1pTENP53fSIW9xWuxtPd6Mzry17E/1JYy2eycXo=]

using Algo [AES/ECB/PKCS5PADDING]

2b7e151628aed2a6abf71589

y con eso hemos obtenido la clave, con la que se puede descifrar el mensaje original:

[decrypt]

[YaSq25Cor+hMTRDDa0mzHA==]

using Algo [AES/CBC/PKCS5PADDING]



Hola, Darius

d) Reflexione sobre si este último modo de compartir la clave es más seguro que el anterior. No, debido a que se sigue teniendo que compartir una clave para descifrar la clave, y si eso se ha podido realizar, no existe ninguna diferencia con descifrar directamente el mensaje con la clave o descifrar la clave con la clave.

Criptografía Asimétrica

Entrando en la página [web](#):

Primero se generan las claves:

Generate RSA Key Online

Select RSA Key Size

1024 bit

Generate RSA Key Pair

Public Key

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCRZcpIKjdy6VPnw+CcETPs8jOv5wfAxxDCLVqa9+qv4p15WZLbivYDFp3ftdI4QKSMLO1TSDIFZbGQ93IfWxDFUronyfbleJTWVZtT4rbsxq65wGweW5ir6hwNCzhxTWsOeGYGuT7f+lqsy9dzoSeUPot/NLi8aa0p47fcVoSpwIDAQAB
```

Private Key

```
BaUuLCfH8lp182ZYmgxAkBeSbV6RFOzXAem2ihvGTD0kLQYuRQIU2ZPqDwtVgzQOJPqOlw7PI9yZ6xlCpwSq28Pq0pfQ3r3x5NNZrVYgCxAkB4TN1U3EH0clOuYgYTThZDP8EqNlajLznuj6EzLf75Blf7aD9QI2svPSyXq1pr1b2tLVSt5hDFhjv4TvnvoA2m
```

Después se encripta el mensaje con la clave pública generada.

RSA Encryption

Enter Plain Text to Encrypt

Hola Darius

Enter Public/Private key

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCRZcpIKjdy6VPnw+CcETPs8jOv5wfAxxDCLVqa9+qv4p15WZLbivYDFp3ftdI4QKSMLO1TSDIFZbGQ93IfWxDFUronyfbleJTWVZtT4rbsxq65wGweW5ir6hwNCzhxTWsOeGYGuT7f+lqsy9dzoSeUPot/NLi8aa0p47fcVoSpwIDAQAB
```

RSA Key Type: ☒ Public key ☐ Private Key

Select Cipher Type

RSA/ECB/PKCS1Padding

Encrypt

Y una vez generado el mensaje, se puede descifrar con la clave privada obteniendo el mensaje.

RSA Decryption

Enter Encrypted Text to Decrypt (Base64)

DYpWYcDI2XPHrdgPTjslyOJzxuweW4FIEFyMZ
XdfLiVWq35QwkJZyMuKX8kb17ZW7yj4bO7fN
/ypJIZlbcB1rmxacjvfvhAZbYUxG0xFkkMou5b
gQ0d

Enter Public/Private key

BaUuLCfH8lpI82ZYmgxAkBeSbV6RFOzXAem
2ihvGTD0kLQYuRQIU2ZPqDwtVgzQOJPqOlw
7PI9yZ6xlCpwSq28Pq0pfQ3r3x5NNZrVYgCxA
kB4TN1U3EH0clOuYgYTThZDP8EqNIajLznuj6Ez
Lf75BIf7aD9QI2svPSyXqIpr1b2tLVSt5hDFhJv4T
vnvoA2m

RSA Key Type: ☐ Public key ☒ Private Key

Select Cipher Type

RSA/ECB/PKCS1Padding

Decrypt

Decrypted Output:

Hola Darius