

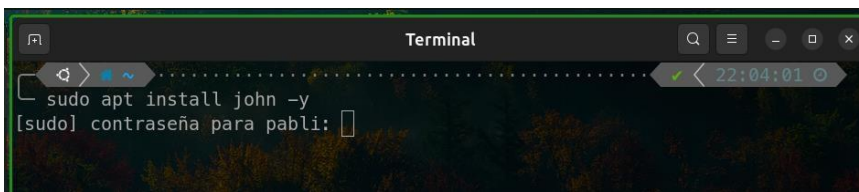
Práctica Criptografía SSI

UO282440

Pablo José Pérez Díez

Paso 1:

Instalo john the ripper:

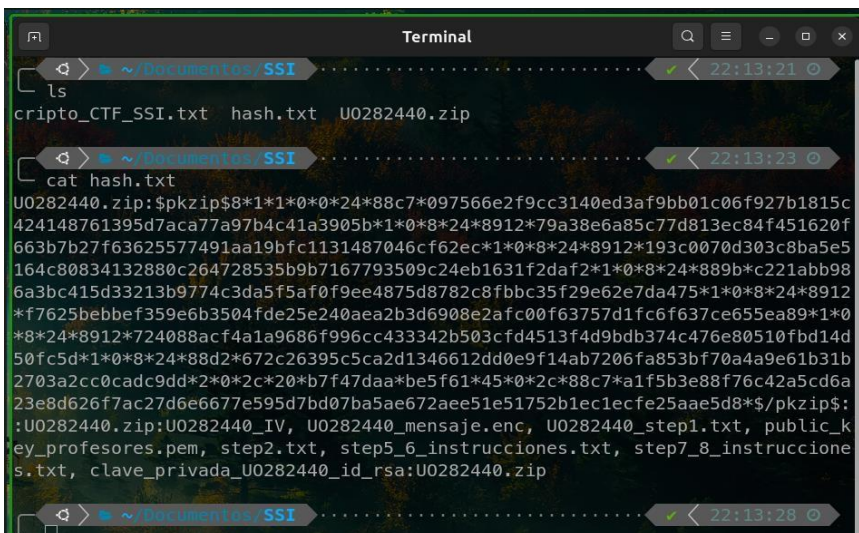


```
Terminal
[~] > sudo apt install john -y
[sudo] contraseña para pabli: [ ]
```

Obtengo el hash del zip:



```
Terminal
[~] > john-the-ripper.zip2john UO282440.zip > hash.txt
```



```
Terminal
[~] > ls
cripto_CTF_SSI.txt  hash.txt  UO282440.zip

[~] > cat hash.txt
UO282440.zip:$pkzip$8*1*1*0*0*24*88c7*097566e2f9cc3140ed3af9bb01c06f927b1815c
424148761395d7aca77a97b4c41a3905b*1*0*8*24*8912*79a38e6a85c77d813ec84f451620f
663b7b27f63625577491aa19bfc1131487046cf62ec*1*0*8*24*8912*193c0070d303c8ba5e5
164c80834132880c264728535b9b7167793509c24eb1631f2daf2*1*0*8*24*889b*c221abb98
6a3bc415d33213b9774c3da5f5af0f9ee4875d8782c8fbbc35f29e62e7da475*1*0*8*24*8912
*f7625bebbef359e6b3504fde25e240aea2b3d6908e2afc00f63757d1fc6f637ce655ea89*1*0
*8*24*8912*724088acf4a1a9686f996cc433342b503cfd4513f4d9bdb374c476e80510fbd14d
50fc5d*1*0*8*24*88d2*672c26395c5ca2d1346612dd0e9f14ab7206fa853bf70a4a9e61b31b
2703a2cc0cad9dd*2*0*2c*20*b7f47daa*be5f61*45*0*2c*88c7*a1f5b3e88f76c42a5cd6a
23e8d626f7ac27d6e6677e595d7bd07ba5ae672aee51e51752b1ec1ecfe25aae5d8*$/pkzip$:
:UO282440.zip:UO282440_IV, UO282440_mensaje.enc, UO282440_step1.txt, public_k
ey_profesores.pem, step2.txt, step5_6_instrucciones.txt, step7_8_instruccione
s.txt, clave_privada_UO282440_id_rsa:UO282440.zip
```

Durante el desarrollo de esta práctica decidí cambiar de sistema operativo en ciertos pasos para no tener que instalar herramientas o software adicional en mi máquina anfitrión, usando así, una máquina virtual (kali) con todas las herramientas que necesitare utilizar durante la práctica.

Como nos dijeron que la contraseña tiene máximo 6 caracteres y está formada solo por letras (mayúsculas/minúsculas) y números, usaremos el modo incremental optimizado:

```
(pabli@kali)-[~/Downloads]
$ john --incremental=alnum --max-length=6 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

El proceso acaba y obtenemos la contraseña: **dCqtf**

```
$ john --incremental=alnum --max-length=6 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
dCqtf
(U0282440 1.zip)
1g 0:00:11:17 DONE (2025-02-20 23:15) 0.001475g/s 18737Kp/s 18737Kc/s 18737Kc/s dChjB..pKA4q
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

El mensaje final de la etapa 1 es: e7Hcx

```
~/Downloads/U0282440 1/U0282440_step1.txt - Mousepad
File Edit Search View Document Help
1 Este archivo es para el estudiante U0282440.
2
3 Mensaje que tienes que subir en las respuestas: Your message is e7Hcx
```

Paso 2:

Buscamos los hashes de las imágenes para ver de qué imagen se trata:

```
$ ls
U0282440_IV          clave_privada_U0282440_id_rsa  image_2.jpg  public_key_profesores.pem  step7_8_instr
U0282440_mensaje.enc image_0.jpg                    image_3.jpg  step2.txt
U0282440_step1.txt  image_1.jpg                    image_4.jpg  step5_6_instrucciones.txt

(pabli@kali)-[~/Downloads/U0282440 1]
$ sha1sum *.jpg
0e81f4742b444076f2bf65d4c2f54be493c8f5be  image_0.jpg
85763e78a68cf4d9c8dc7dbdb7bee1bc8efe07cc  image_1.jpg
cfc2b8bddb97f7fd595a5a2c57319b8cf583f3fe  image_2.jpg
0d92e7407b0e0bd4edae586c2784248989012a27  image_3.jpg
b3a8e0ea4ec56e51308bd8ccfb53b8b4d312b5ca  image_4.jpg
```

Finalmente obtenemos la imagen usando sha224sum después de varios intentos con otros algoritmos.

```
(pabli@kali)-[~/Downloads/U0282440 1]
$ sha224sum *.jpg | grep 7d56d8786c1b96788cf6fa0670062792ca859b5ad26536154434a0e9
7d56d8786c1b96788cf6fa0670062792ca859b5ad26536154434a0e9  image_2.jpg
```

Obtenemos las palabras de posibles contraseñas:

```
wget http://156.35.163.140:777
--2025-02-21 13:40:30-- http://156.35.163.140:777/
Conectando con 156.35.163.140:777... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 39084 (38K) [text/html]
Guardando como: 'index.html'

index.html      100%[=====] 38,17K  --.-KB/s   en 0,06s

2025-02-21 13:40:30 (618 KB/s) - 'index.html' guardado [39084/39084]
```

Meto las palabras del html en un txt para utilizarlo usando lynx:

```
(pabli@kali)-[~/Downloads/U0282440 1]
$ lynx -dump http://156.35.163.140:777 | tr ' ' '\n' | sort -u > palabras_lynx.txt

(pabli@kali)-[~/Downloads/U0282440 1]
$ ls
U0282440_IV                image_0.jpg  image_4.jpg  public_key_profesores.pem
U0282440_mensaje.enc       image_1.jpg  index.html   step2.txt
U0282440_step1.txt         image_2.jpg  palabras.txt  step5_6_instrucciones.txt
clave_privada_U0282440_id_rsa image_3.jpg  palabras_lynx.txt step7_8_instrucciones.txt
```

Usando stegcracker y la lista de palabras anterior obtenemos la contraseña: **Enlaces**

```
(pabli@kali)-[~/Downloads/U0282440 1]
$ stegcracker image_2.jpg palabras_lynx.txt

StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2025 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'image_2.jpg' with wordlist 'palabras_lynx.txt'..
Successfully cracked file with password: Enlaces
Tried 286 passwords
Your file has been written to: image_2.jpg.out
Enlaces
```

Obtenemos el mensaje:

```
(pabli@kali)-[~/Downloads/U0282440 1]
$ cat image_2.jpg.out
Has conseguido obtener un mensaje ¿será el correcto?...
INSTRUCCIONES PASOS 3 y 4.
A continuación te damos una clave que te servirá para descryptar el fichero U0XXXXX_encryptado que has obtenido al descomprimir el fichero zip
1e0384be8389918020b55c3e0ed246
el siguiente paso consiste en descryptar ese mensaje. Tendrás que probar con distintos algoritmos de los que mencionamos en las instrucciones.
Además, una vez que hayas descryptado el mensaje probablemente no seas capaz de entenderlo ya que estará codificado con alguno de los algoritmos
que mencionamos en las instrucciones.
El mensaje será una pregunta muy sencilla.
Lo que debes subir en la web de respuestas es el mensaje descryptado, pero sin decodificar, además el mensaje decodificado y por último, la respuesta
a la pregunta que te hacemos, que será un número.

You have managed to retrieve a message. Could it be the correct one?
INSTRUCTIONS - STEPS 3 & 4
We are providing you with a key that will allow you to decrypt the file 1904+077 _encryptado, which you obtained after extracting the ZIP file
1e0384be8389918020b55c3e0ed246
The next step is to decrypt this message. You will need to experiment with different algorithms mentioned in the instructions. Additionally, once
you have decrypted the message, you may not be able to understand it, as it will be encoded using one of the encoding methods also mentioned in
the instructions.
The message will contain a very simple question.
You must upload the following to the response website: The decrypted message, but still encoded. The decoded message. The answer to the question
in the message (which will be a number).
```

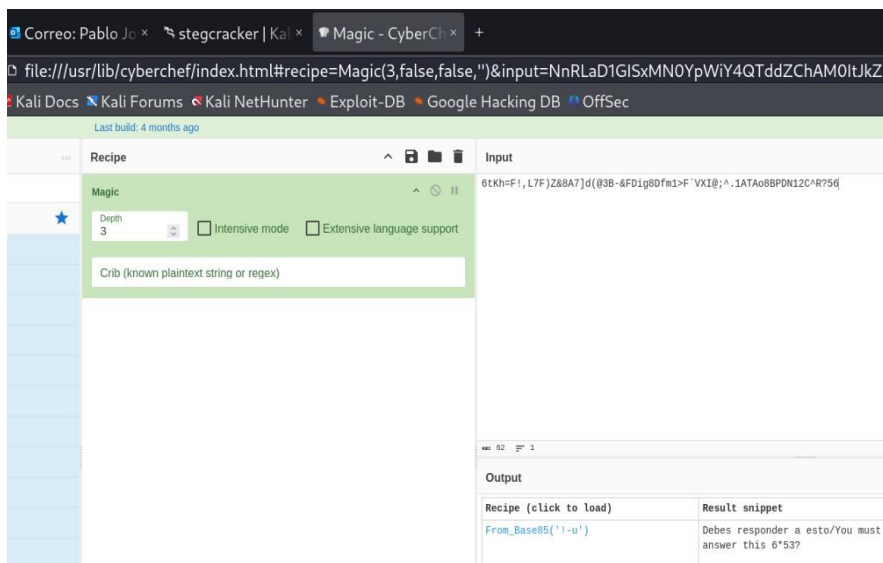
Pasos 3 y 4:

Mensaje descifrado:

```
(pabli@kali)-[~/Downloads/U0282440 1]
$ openssl enc -aes-256-cbc -d -in U0282440_mensaje.enc -out mensaje_descifrado.txt \
-K 1e0384be8305918020b655c3e06de54600000000000000000000000000000000 \
-iv a9128f781245e2cf82742aa0a814e9bf

(pabli@kali)-[~/Downloads/U0282440 1]
$ cat mensaje_descifrado.txt
6tKh=F!,L7F)Z68A7]d(@3B-8FDig8Dfm1>F`VXI@;^1ATAo8BPDN12C^R?56
```

Utilizando cyberchef decodificamos el mensaje y obtenemos la pregunta:



Paso 5:

Me conecto a la máquina mediante ssh:

```

[~]
U0282440@3df155d5abcf:~
d ~ - ssh -i clave_privada_U0282440_id_rsa -p 2222 U0282440@156.35.163.140
ssh -i clave_privada_U0282440_id_rsa -p 2222 U0282440@156.35.163.140

The authenticity of host '[156.35.163.140]:2222 ([156.35.163.140]:2222)' can't be established.
ED25519 key fingerprint is SHA256:9Rq1FI4NY0m5EuCVaju8fOs+0DTc9svqeu3kmUThL0g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[156.35.163.140]:2222' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Acceso con éxito a tu cuenta U0282440 mediante certificado
02834f1007463155d5abcf.6

```


Obtenemos la clave del paso 5:

```
U0282440@3df155d5abcf:~$ ls -la
total 44
drwxr-xr-x  4 U0282440 U0282440 4096 Feb 22 19:34 .
drwxr-xr-x  1 root    root      12288 Feb 10 16:11 ..
-rw-r--r--  1 U0282440 U0282440  220 Mar 31 2024 .bash_logout
-rw-r--r--  1 U0282440 U0282440 3838 Feb 10 16:11 .bashrc
drwx----- 2 U0282440 U0282440 4096 Feb 22 19:34 .cache
-rw-r--r--  1 U0282440 U0282440  807 Mar 31 2024 .profile
drwx----- 2 U0282440 U0282440 4096 Feb 10 16:11 .ssh
-rw-----  1 U0282440 U0282440   65 Feb 10 16:11 local_hash
-rw-r--r--  1 root    root       11 Feb 10 16:11 respuesta_U0282440_step5
U0282440@3df155d5abcf:~$ cat respuesta_U0282440_step5
YVP0131aCZ
U0282440@3df155d5abcf:~$
```

Paso 6:

Nos bajamos el hash a nuestra maquina local:

```
> Do SS /U0282440_descomprimido_ssi/U0282440 1 20:57:32
scp -P 2222 -i clave_privada_U0282440_id_rsa U0282440@156.35.163.140:local_hash .
local_hash 100% 65 1.6KB/s 00:00
> Do SS /U0282440_descomprimido_ssi/U0282440 1 20:58:41
ls
clave_privada_U0282440_id_rsa public_key_profesores.pem
image_0.jpg step2.txt
image_1.jpg step5_6_instrucciones.txt
image_2.jpg step7_8_instrucciones.txt
image_3.jpg U0282440_IV
image_4.jpg U0282440_mensaje.enc
local_hash U0282440_step1.txt
> Do SS /U0282440_descomprimido_ssi/U0282440 1 20:58:43
cat local_hash
f67f3cabf8faa33c7e7c4d0910127603343584d78fc0c6d54a64375250ff3548
```

Identificamos los posibles algoritmos utilizados en el hash con hashid:

```
pabli@CNI: ~/Documentos/SSI/U0282440_descomprimido_ssi/U0282440 1
> Do SS /U0282440_descomprimido_ssi/U0282440 1 21:15:20
hashid local_hash
--File 'local_hash'--
Analyzing 'f67f3cabf8faa33c7e7c4d0910127603343584d78fc0c6d54a64375250ff3548'
[+] Snefru-256
[+] SHA-256
[+] RIPEMD-256
[+] Haval-256
[+] GOST R 34.11-94
[+] GOST CryptoPro S-Box
[+] SHA3-256
[+] Skein-256
[+] Skein-512(256)
--End of file 'local_hash'--
```

Obtenemos la contraseña usando crackstation:

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
f67f3cabf8faa33c7e7c4d0910127603343584d78fc0c6d54a64375250ff3548	sha256	cyclobentadienyl-ruthenium

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

[Download CrackStation's Wordlist](#)

Y entramos en el usuario:

```
U0282440@3df155d5abcf:~$ su local_U0282440
Password:
local_U0282440@3df155d5abcf:/home/U0282440$ whoami
local_U0282440
local_U0282440@3df155d5abcf:/home/U0282440$
```

Obtenemos el token:

```
local_U0282440@3df155d5abcf:/home/U0282440$ cd
local_U0282440@3df155d5abcf:~$ ls
token
local_U0282440@3df155d5abcf:~$ cat token
WN4S6qgpslzABusPLeJv5yuWF6S94mkzPZupvAWSmHT0cv8hhx
local_U0282440@3df155d5abcf:~$
```

Paso 7:

Generamos clave para el certificado:

```
~/Documentos/SSI ..... 18:57:30
$ openssl genkey -algorithm RSA -out clave_privada.key
.....
.....*.....
.....
```

Genero solicitud de certificado:

```
~/Documentos/SSI ..... 18:57:30
$ openssl req -new -key clave_privada.key -out solicitud.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Asturias
Locality Name (eg, city) []:Oviedo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:localhost
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:localhost
Email Address []:uo282440@uniovi.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:2a4b6c7d
An optional company name []:
```

Subo csr al servidor y descargo la firma:

← → ↻ ⚠ No es seguro 156.35.163.140:5000 📄 ☆ ⬇️ (P) Reiniciar

Subir CSR para Firma

Seleccionar archivo CSR: solicitud.csr

Paso 8:

Cifro el archivo token con la clave pública:

```
~/.Documentos/SSI ..... 19:12:56
openssl pkeyutl -encrypt -pubin -inkey public_key_profesores.pem -in token_paso_6 -out token_cifrado.bin

~/.Documentos/SSI ..... 19:13:22
ls
clave_privada.key      solicitud.csr
contraseña_usuario_paso_6 solicitud_signed.pem
cripto_CTF_SSI.txt     token_cifrado.bin
hash Og.txt            token_paso_6
hash.txt               U0282440_descomprimido_ssi
memoriaCriptografia.odt U0282440_descomprimido_ssi.zip
public_key_profesores.pem U0282440.zip
respuesta_U0282440_step5
```

Firmo el archivo con mi certificado:

```
~/.Documentos/SSI ..... 19:15:14
openssl dgst -sha256 -sign clave_privada.key -out firmado_por_mi_token.sig token_cifrado.bin
```

Por último, envío todas las respuestas a la web:

```
Curso: Seguridad x ES. Lab 03-04. Cript x Correo: Pablo Jo x 156.35.163.140:44 x
https://156.35.163.140:444/2af33cc0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Subida exitosa para U0282440!
Fecha y hora de subida: 2025-02-23 19:37:48
Campos enviados: { 'field1': 'dCqtf', 'field2': 'e7Hcx', 'field3': 'image_2.jpg', 'field4': 'Enlaces', 'field5': '1e0384be8305918020b655c3e06de546', 'field6': 'AES 256 CBC', 'field7': '6tKh=FI,L7FJZ&8A7jd@3B-&FDig8Dfm1>F VXi@;^1ATAo8BPDN12C^R?56', 'field8': 'Base85', 'field9': 'Debes responder a esto/you must answer this 6*53?', 'field10': '318', 'field11': 'VVP0131aCZ', 'field12': 'f673cab8faa33c7e7c4d0910127603343584d78f0c6d54a64375250ff3548', 'field13': 'cyclobentadienyl-ruthenium', 'field14': 'WN4S6gqslzABusPLejv5yuWF6S94mkzPZupvAWSmHTOCv8hxx' }
Archivos subidos:
- file1: token_cifrado.bin (d80c7735c36fb9cd6fb136e635a734acb86bfc1c8ede808eadca80e010e17a53)
- file2: solicitud_signed.pem (12779cb98b5ff1c4c0c2fd95da362da37b2d260a733673e93467a05ca0b78bb)
- file3: solicitud.csr (d4e0ca87a5f04e8e64bc8a6020315f6de4c458b76b31e590d0b95ec3f177bdc8)
```