

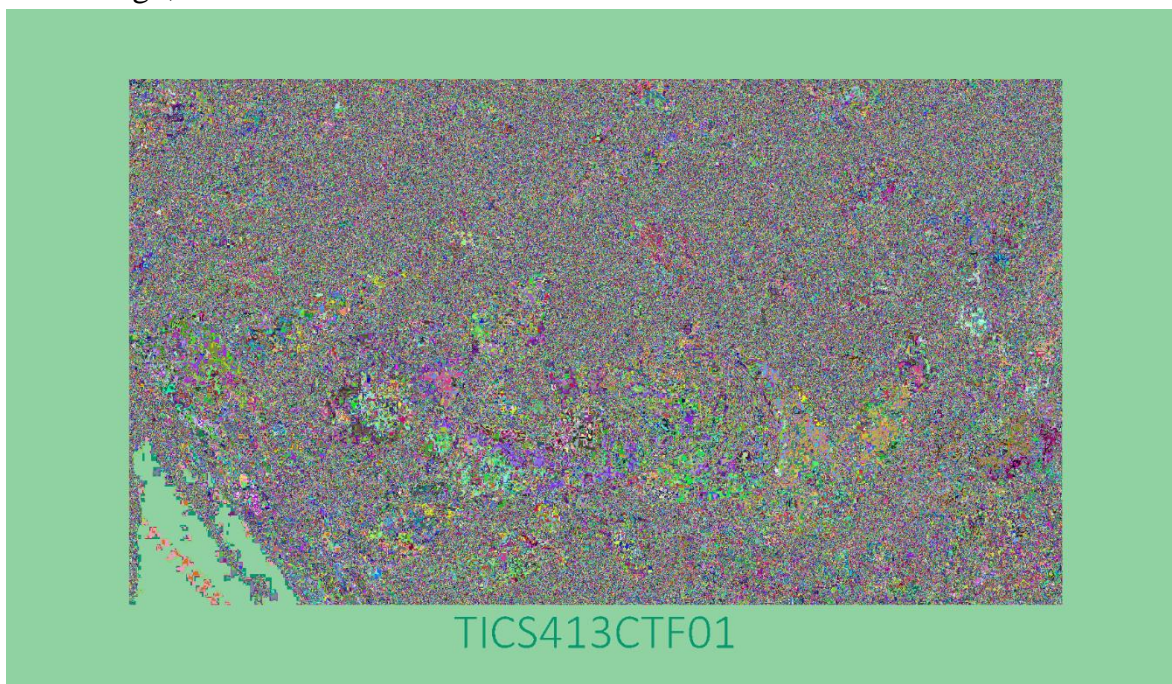


CTF 01

2-2023

Estudiante: Nicolás Soto
Profesor: Nicolás Cenzano

Primero, recordamos la pregunta que se nos hizo en el laboratorio, que nos daba una hint de había que usar Cyberchef para decifrar algún tipo de contraseña. Buscamos en Cyberchef “Randomize Colour Palette” y ponemos la imagen que se nos entregó, obtendremos esto.



Con la inteligencia recolectada, asumimos que el mensaje descubierto es la contraseña del pdf. Al colocarlo, obtenemos esta información.

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z442Kgf4f0ZnHsBw43gfyeBTtBS3GStnlBv1Ff+IfzT
pNihPvuXguV/JsecBhP2MvqCR0C2LwinTWZlxBy9Hq7KXKhTRVbheBAc3IQHgJpy
PWcGv6EzPHRwgpGKP1B470ZCx8IvGVrcJUedw1BowRPDCj4mYU7I0ihnAgMBAAEC
gYAQtiEcUNgnfGGsCtPrEPe/Z2bX2+ZsidommxXo57T/Ph4e3XXlvNAZFHlyytK
nd1nRJf30aoPzEaZJbtIFSkrrnGu7ARpbHAY+YGzILSrSM3Hs7FNFLFH83pu5JuFn
80KvpHp+y7y2jAazLA6oqdvKL3+i2i2a/9E34uuGEijggQJBALtXfgWk9QJ0g9Fb
mGbzc6c0bUAcM6jzLBIAEbuS9Pfh+bNpFLVnvSEaz7hVvC1d4QJIqzaHZy1chVbE
JUToticCQQCUKeDelbninpe+E2T2+4qV1x4/vv5nUSuLFLA0PAR069nrKfsV7RM
jSkjG5iWSPvTXf9meRsS7FrBfKVhKqPBAKEAt+8yCyana8lcwLwWIRXz8jGWJkDK
M9JbE00HxYuGuq4CtLSzucyts4gYc9qxdDVdCxoAB/yvP6k8PTE9ikeVNwJAPQy0
d4LCQTqP0+Yx6ALq7Aj6qhMM2oyDq1XG9P71138fH+MAbpxtElF9g1c5i/Uc9d7
cUHDggKZsrglfNARAQJAXijomQyphaLvNLLqPKChxku8nHR/0hSPBE9LLoB1McY7
em4ovUoGT7t/7zQtD2QSA+D7T/ZeoJnVScB1SgAx9w==
-----END RSA PRIVATE KEY-----
-----BEGIN PUBLIC KEY-----
MIGEMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgGxtOm3j+z442Kgf4f0ZnHsBw43g
fyeBTtBS3GStnlBv1Ff+IfzTpNihPvuXguV/JsecBhP2MvqCR0C2LwinTWZlxBy9
Hq7KXKhTRVbheBAc3IQHgJpyPWcGv6EzPHRwgpGKP1B470ZCx8IvGVrcJUedw1Bo
wRPDCj4mYU7I0ihnAgMBAAE=
-----END PUBLIC KEY-----
```

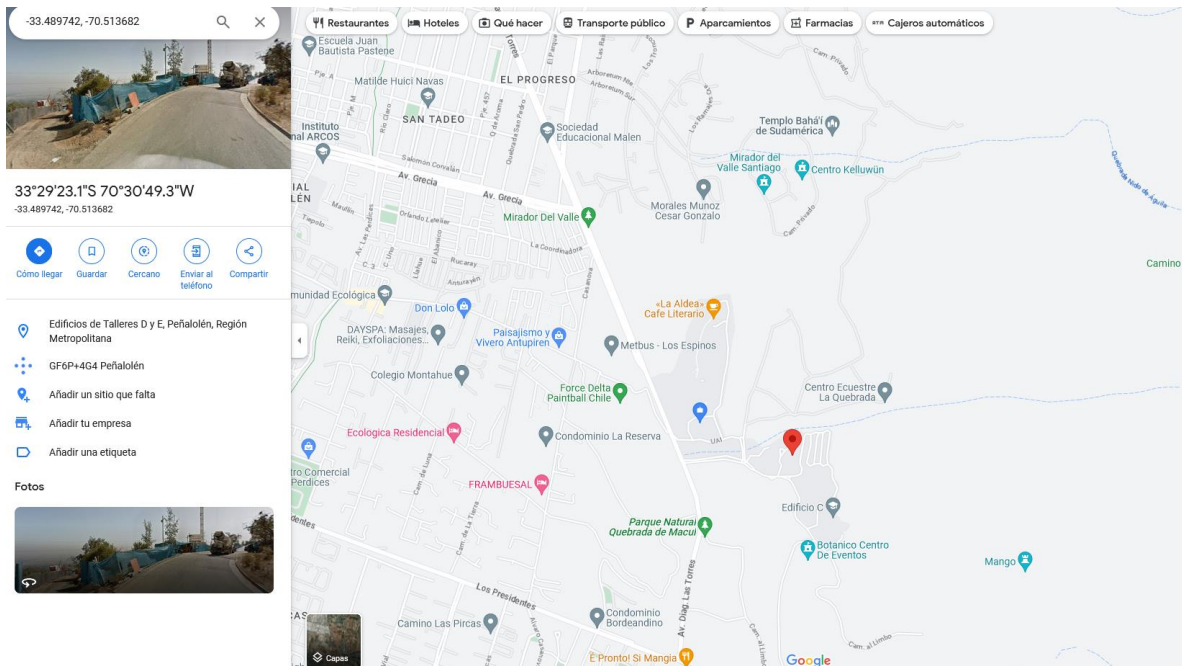
Con las llaves, podemos decifrar el archivo CTF01-coordenadas-iniciales.dat en cyberchef de la siguiente manera:

The screenshot shows the CyberChef interface. On the left, the 'RSA Decrypt' tool is configured with an RSA Private Key (PEM) and the Message Digest Algorithm set to SHA-1. The key text is:
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z442KgF4f0ZnHsBw43gfyeBttB53GStn1Bv1
FF+IzZ1
pN10PvUuGuV/JsecBhP2MvqCR0C2LwintWZLxBy9Hq7KXKhTRVbheBac3

The encryption scheme is RSA-OAEP. The output of the decryption is displayed in the 'Output' tab:
-33.489742, -70.513682

Estas coordenads nos llevan hacia la UAI

<https://www.google.com/maps/place/33%C2%B029'23.1%22S+70%C2%B030'49.3%22W/@-33.4849684,-70.5215061,15.25z/data=!4m4!3m3!8m2!3d-33.489742!4d-70.513682?entry=ttu>



Para lograr el CTF, vamos a RSA ENCRYPT y ponemos coordenadas más familiares para el receptor del documento. Posteriormente descargamos el archivo.

Recipe

RSA Decrypt

RSA Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z44ZKgf4f0ZnHsBw43gfyebTtBS3GStn1Bv1
Ff+IzI
pU1hPvUxguV/JsecBhP2MvqCR0C2Lw1nTWZ1xBy9Hq7KXKhTRVbheBAc3
-----END RSA PRIVATE KEY-----
```

Key Password

Encryption Scheme: RSA-OAEP

Message Digest Algorithm: SHA-1

RSA Encrypt

RSA Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z44ZKgf4f0ZnHsBw43gfyebTtBS3GStn1Bv1
Ff+IzI
pU1hPvUxguV/JsecBhP2MvqCR0C2Lw1nTWZ1xBy9Hq7KXKhTRVbheBAc3
-----END RSA PRIVATE KEY-----
```

Key Password

Encryption Scheme: RSA-OAEP

Message Digest Algorithm: SHA-1

Input

1: CTF01.png X 2: CTF01-coordenadas-iniciales.dat X 3: download.dat X

-33.43687654264965, -70.57311247402595

File details

Name: CTF01-coordenadas-iniciales.dat
Size: 128 bytes
Type: unknown
Loaded: 100%

Output

total: 3
time: 614ms
average: 12ms

< 1: 'HkU'a80X4U'Â0iK6AM*U'HQn±[Ñ#;A[L... 2: >VæOqyQp+WâTjI Ø*Ó(z+;gÑæuÖe"... 3: RSAES-OAEP input message length (192) L... >

>VæOqyQp+WâTjI Ø*Ó(z+;gÑæuÖe"... 2: >VæOqyQp+WâTjI Ø*Ó(z+;gÑæuÖe"... 3: RSAES-OAEP input message length (192) L...

Y por último confirmamos con el decrypt que todo hay salido bien.

Recipe

RSA Decrypt

RSA Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z44ZKgf4f0ZnHsBw43gfyebTtBS3GStn1Bv1
Ff+IzI
pU1hPvUxguV/JsecBhP2MvqCR0C2Lw1nTWZ1xBy9Hq7KXKhTRVbheBAc3
-----END RSA PRIVATE KEY-----
```

Key Password

Encryption Scheme: RSA-OAEP

Message Digest Algorithm: SHA-1

RSA Encrypt

RSA Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z44ZKgf4f0ZnHsBw43gfyebTtBS3GStn1Bv1
Ff+IzI
pU1hPvUxguV/JsecBhP2MvqCR0C2Lw1nTWZ1xBy9Hq7KXKhTRVbheBAc3
-----END RSA PRIVATE KEY-----
```

Key Password

Encryption Scheme: RSA-OAEP

Message Digest Algorithm: SHA-1

Input

1: CTF01.png X 2: CTF01-coordenadas-iniciales.dat X 3: download.dat X

-33.43687654264965, -70.57311247402595

File details

Name: download.dat
Size: 128 bytes
Type: unknown
Loaded: 100%

Output

total: 3
time: 614ms
average: 12ms

< 1: 'HkU'a80X4U'Â0iK6AM*U'HQn±[Ñ#;A[L... 2: >VæOqyQp+WâTjI Ø*Ó(z+;gÑæuÖe"... 3: RSAES-OAEP input message length (192) L... >

>VæOqyQp+WâTjI Ø*Ó(z+;gÑæuÖe"... 2: >VæOqyQp+WâTjI Ø*Ó(z+;gÑæuÖe"... 3: RSAES-OAEP input message length (192) L...