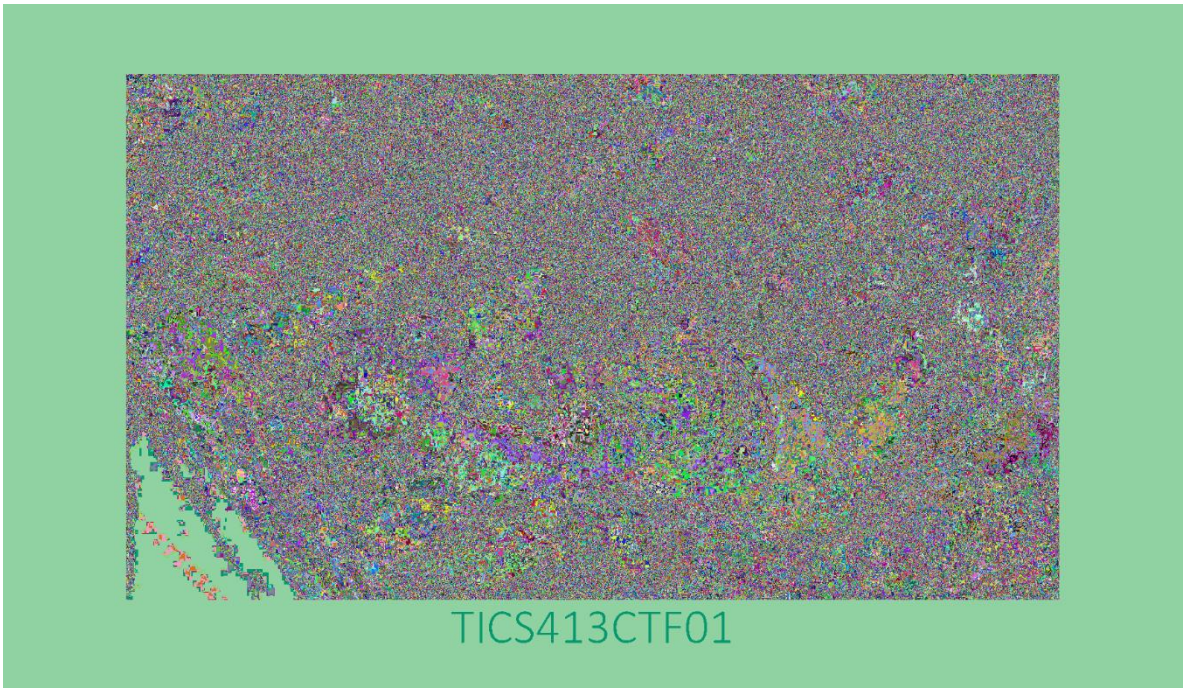
CTF 01
2-2023

Estudiante: Nicolás Soto
Profesor: Nicolás Cenzano

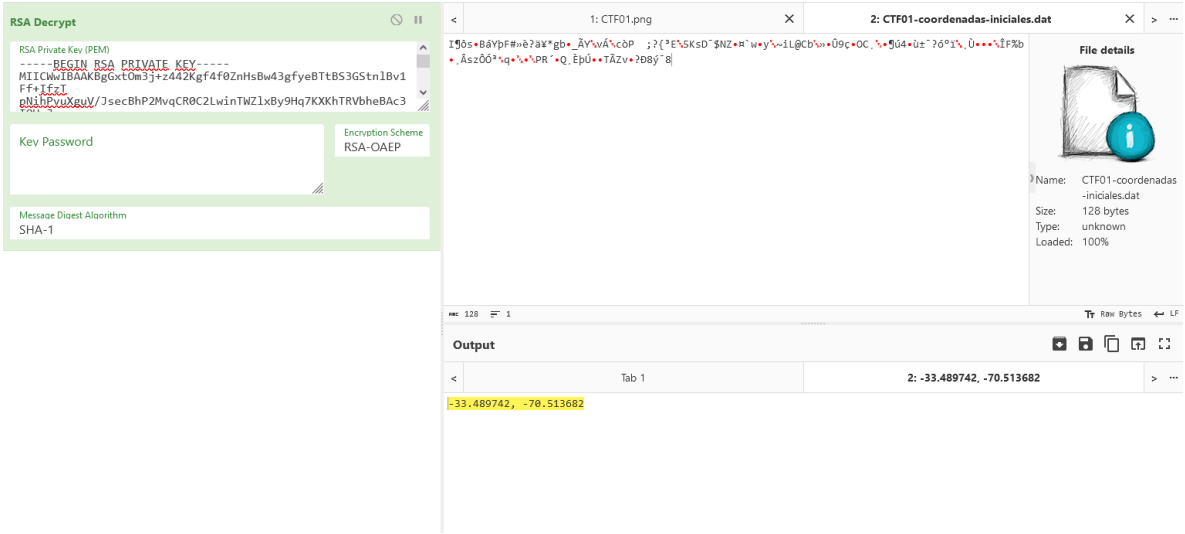
Primero, recordamos la pregunta que se nos hizo en el laboratorio, que nos daba una hint de había que usar Cyberchef para decifrar algún tipo de contraseña.
Buscamos en Cyberchef “Randomize Colour Palette” y ponemos la imagen que se nos entregó, obtendremos esto.



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

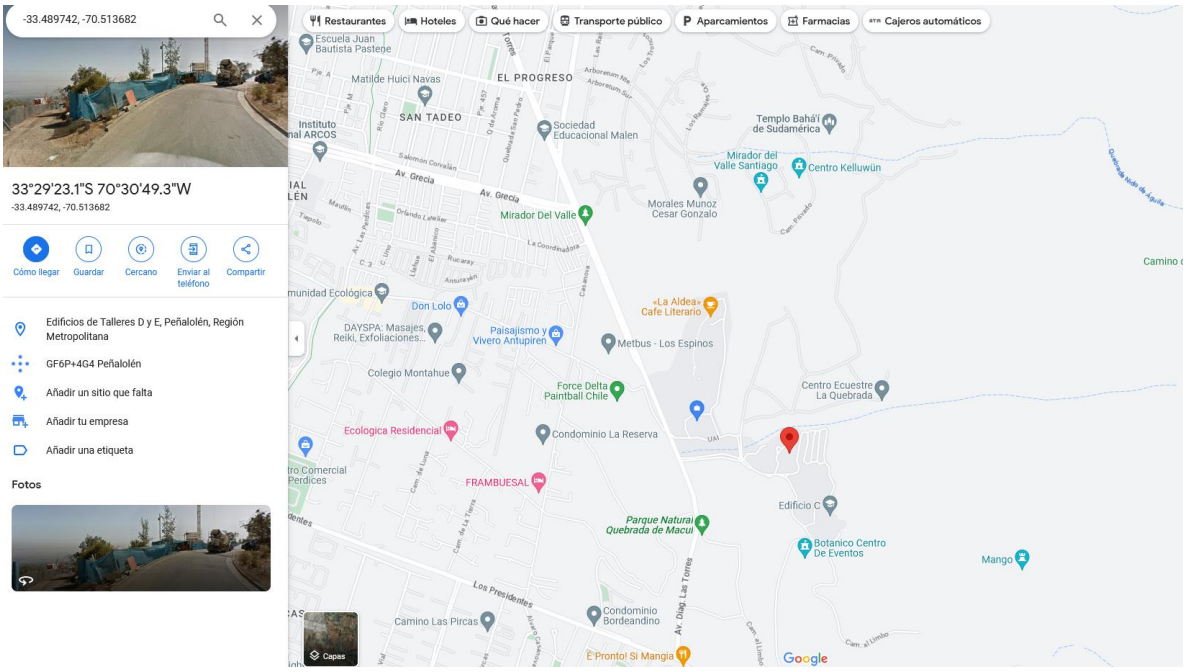
```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z442Kgf4f0ZnHsBw43gfyeBTtBS3GStnlBv1Ff+IfzT
pNihPvuXguV/JsecBhP2MvqCR0C2LwinTWZlxBy9Hq7KXKhTRVbheBAc3IQHgJpy
PWcGv6EzPHRwgpGKP1B470ZCx8IvGVrcJUedw1BowRPDCj4mYU7I0ihnAgMBAAEC
gYAQtiEcUNgndfGGsCtPrEPe/Z2bX2+ZsidommzXo57T/Ph4e3XXlvNAZFHlyytk
nd1nRJf3OaoPzEaZJbtIFSkrnGu7ARPbHAy+YGzILSrSM3Hs7FNFLFH83pu5JuFn
8OKvpHp+y7y2jAazLA6oqdvKL3+i2i2a/9E34uuGEijggQJBALtXfgWk9QJOg9Fb
mGbzc6c0bUAcM6jzlBlAEbuS9Pfh+bNpFlVnvSEaz7hVvC1d4QJIqzaHZy1chVbE
JUToticCQQCUKeDelbninpe+E2T2+4qV1x4/vv5nlUSulFLA0PARO69nrKfsV7RM
jSkjG5iWSPvTXf9meRsS7FrBfKVhKqPBAkEAt+8yCyana8lcwLvWiRXz8jGWJkDK
M9JbEOOHxYuGuq4CtLSzucyts4gYc9qxdDVdCxoAB/yvP6k8PTE9ikeVNwJAPQy0
d4LCQTqP0+Yx6ALlq7Aj6qhMM2oyDq1XG9P71138fH+MAbpxtElF9g1c5i/Uc9d7
cUHdggKZsrglfNARAQJAXijomQyphaLvNLLqPKChxku8nHR/0hSPBE9LLoBlMcY7
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:

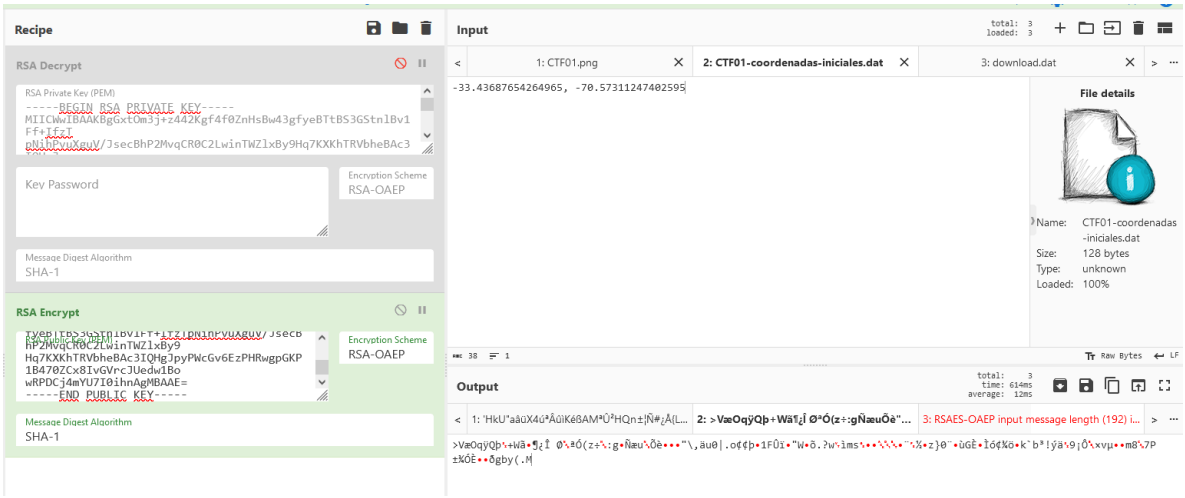


Estas coordenads nos llevan hacia la UAI

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.



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