CT01

Seguridad en TI

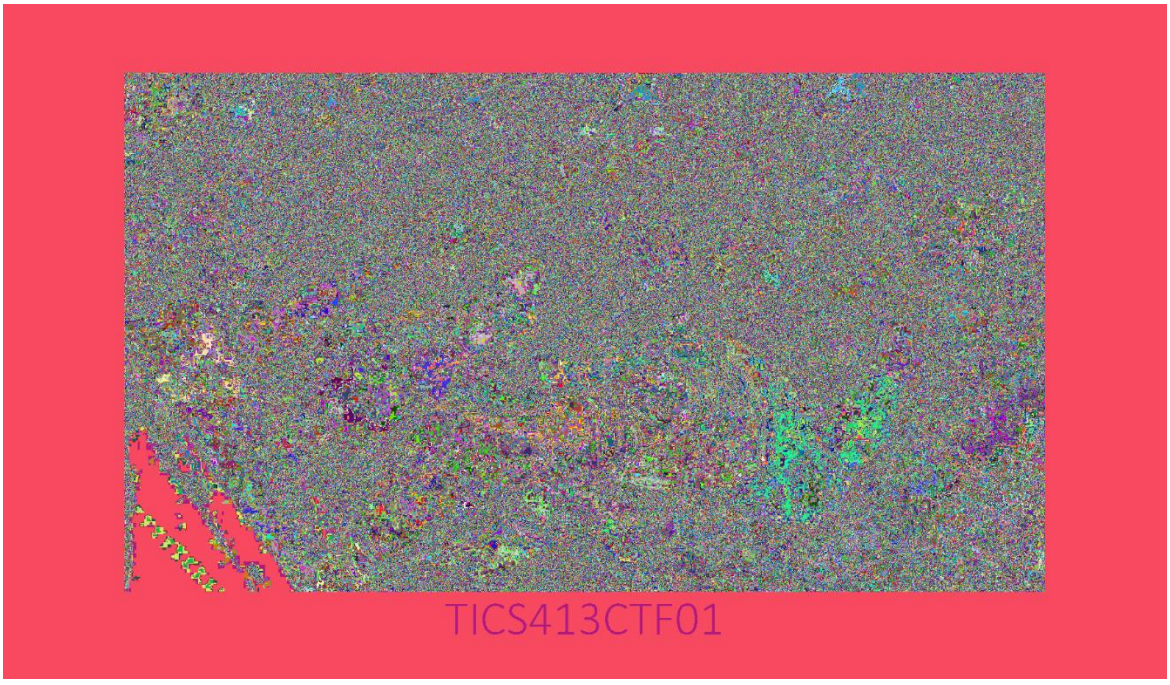
Pedro Fajardo Pérez

Paso 1:

Ingresar a la plataforma Cyberchef, plataforma que me ayudará a descifrar el mensaje de la imagen, a través del uso de las herramientas que ofrece.

Paso 2:

Al ser una imagen lo que se hizo fue buscar las herramientas que ofrece Cyberchef para las imágenes, al buscar img en el buscador, se hizo una prueba con cada una de ellas para encontrar algo que pueda llamar la atención. Al ocupar la llamada “Randomize Colour Palette” pudimos ver que nos dio un output en el cual podemos ver un texto en la parte inferior.



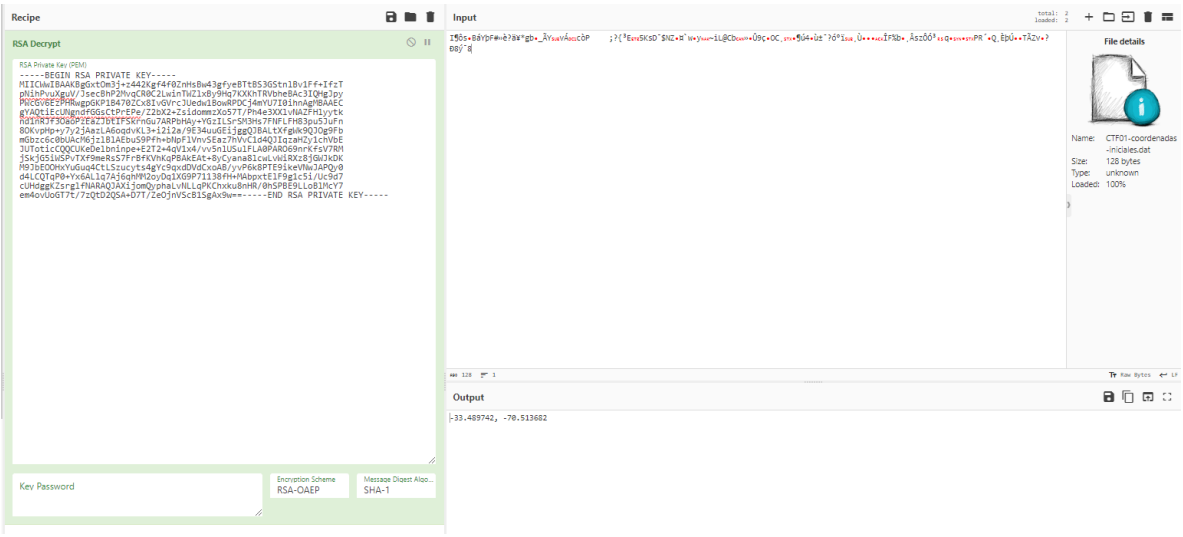
Paso 3:

Al usar ese texto como contraseña en el archivo pdf que estaba bloqueado por una pudimos entrar, mostrando las dos keys (Privada y pública), como también nos entregó información de que fue usado RSA para encriptar el mensaje.

```
-----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-----
```

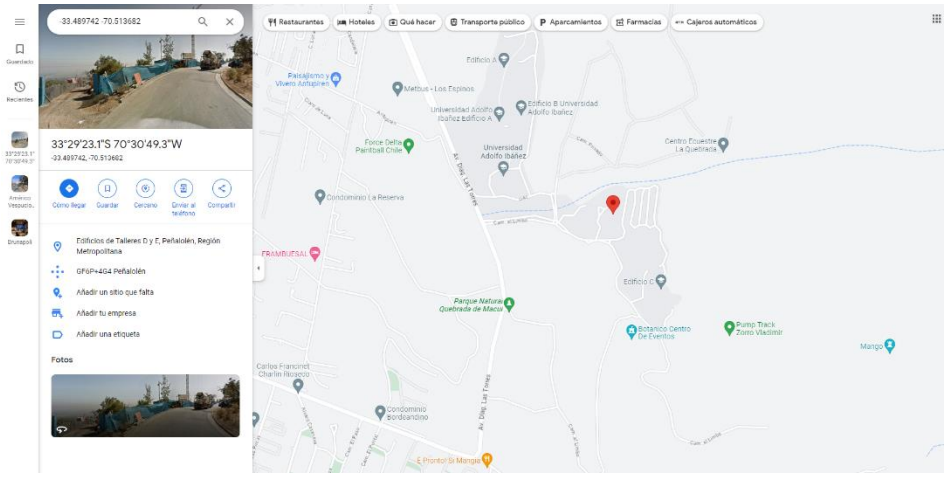
Paso 4:

Al buscar las herramientas de RSA, encontré la llamada “RSA Decrypt”, la cual utilicé para encontrar las coordenadas del archivo .dat entregado



Paso 5:

Las coordenadas nos llevaron al edificio de la D universidad, por lo que ahora tuvimos que elegir unas nuevas coordenadas para la entrega del premio.



Paso 6:

Se hizo un cambio de coordenadas y mediante el uso de “RSA Encrypt” de CyberChef y la llave pública logramos encriptar las nuevas coordenadas en un nuevo archivo .dat