

# Capture the flag N°1:

Alumno: Andrés Guerra

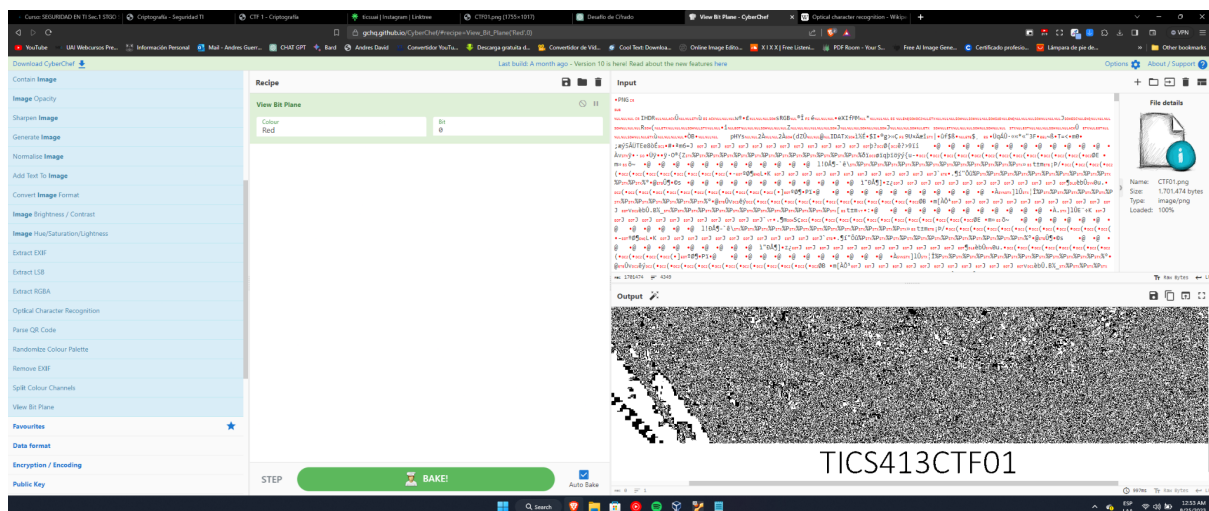
Profesor: Nicolas Cenzano

Curso: Seguridad en TI SEC.1 STGO

## Desarrollo:

### 1) Análisis de la imagen

Mi primer paso fue buscar la clave del PDF dentro de la imagen. Al principio, intenté localizarla visualmente mediante un zoom en la imagen, pero no obtuve resultados. Luego, al notar que los bordes negros de la imagen eran inusuales, invertí los colores para investigar, pero aún así no pude encontrar nada. Después, opté por abrir la imagen en Cyberchef y analizar todas las operaciones relacionadas con imágenes. Para ello, introduje "image" en el buscador. A medida que probaba diferentes operadores, finalmente encontré la solución utilizando "View Bit Plane". Este operador mostraba únicamente un bit de cada píxel, lo cual permitía ocultar mensajes. Fue así como descubrí la clave oculta: TICS413CTF01.



### 2) Obtener public y private key:

Al obtener la contraseña del PDF, este se desbloquea y nos revela la public y private key que sirven para cifrar y descifrar el archivo .dat que tiene la ubicación del premio. Que sería la siguiente:

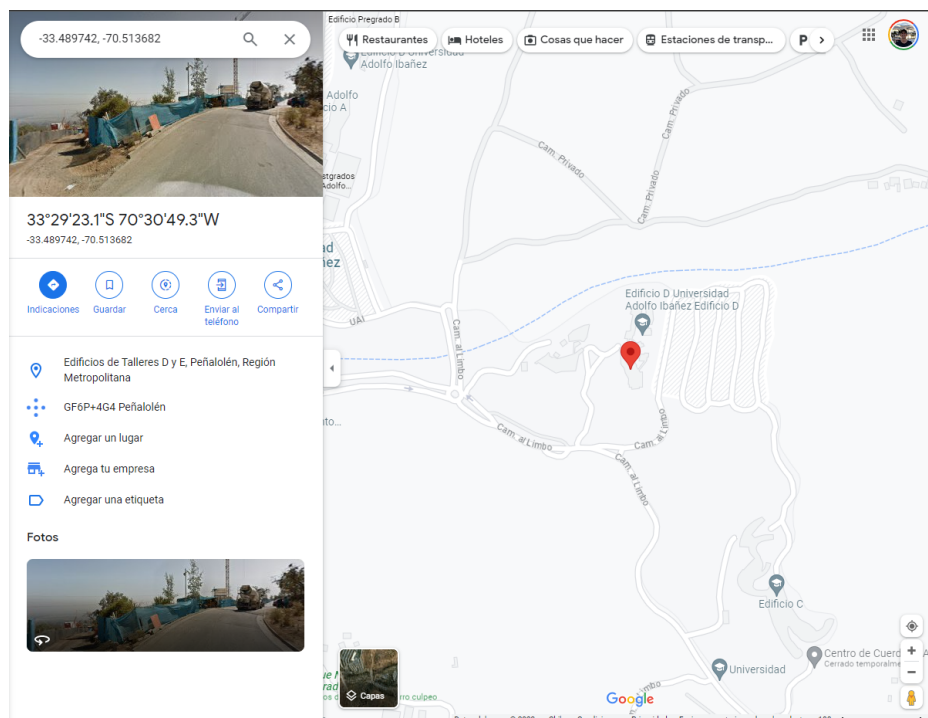
```
-----BEGIN RSA PRIVATE KEY-----
MIICMwI BAAKBgGxtOn3j +z442Kgf4f0ZnHsBu4 3gfyebTtBS3GStnI8v1ff+IzfzT
pN1hPvuXguN/J secBhP2MvqCR0 CZLwinTMZ Lx8Y9Hq7KXXhTRV bheBAC 310HgJ py
PMcGv6E zPHrugpGKP1B4 70ZCx8 IvGVrc JUedw1BoWPRD Cj4nYU 710IhnAgMBAAE
gYAQIIE cUNgnd fGGSctP rEPe/Z 2bX2+Z s idomn zXo57T /Ph4e3XXlvNA ZFHlYy tk
nd1nRj f 30aoPz EaZJbtI FSknnGu7ARpbHay+YG zILs5M3Hs7FNFLFH8 3pu5JuFn
8OKvphp +yy7y2j AazLA6o qdvKL3 +1212a /9E34u uGE1jgqJ8AL txfgMk 9QJog9 Fb
nGbz c6c 06UAcH6j z lB lA Ebu59P fh+Bnp F lVnv5 Eaz7hV vC1d4Q JIqzaH Zy1chV bE
JUTot ic CQQCUK e0e lbn1 npe+E2 T2+4qv 1x4/vv 5n lU5u lFLA0P AR069n rkfsV7 RM
j 5k jG5 i MSPVTX f9meRs5 7FRbfK VhKqPB AKEAt +8yCyan a8 lcuL vM1RXz 8jGMJk DK
M9JbE00 HxYGu q4CtLSz ucyts4 gYc9qxdDVdCxoAB/yv P6k8PT E9ikeVNuJAPQ y0
d4L CQTqP0 +Yx6 AL lq7A j 6qhMM2 oyDq1X G9P711 38fh+M AbpxtE LF9g1c 51/Uc9d7
cUHdgK Zsrg l fNARAQJAX1 jonQ yphaLvNLLqPK Chdku8nHR/0h SPB9L LoB lHc Y7
en4ovUo GT7t/7 zQtdZQS A+07T/ Ze0 jnV ScB1Sg Ax9u==
-----END RSA PRIVATE KEY-----
-----BEGIN PUBLIC KEY-----
MIIGMA0 GCsG5 Ib3DQEB AQUAA4 GMADCB iAKBgG xtOn3j +z442Kgf4f0ZnHsBu4 3g
fyebTtBS 53GStn l8v1ff+ IzfzT pN 1hPvuXguN/J secBhP2MvqCR0 CZLwinTMZ Lx8Y9
Hq7X0Kh TRVbhe BAC310HgJpyPM cGv6Ez PHrugpGKP1B4 70ZCx8 IvGVrc JUedw1Bo
wPRD Cj4nYU710IhnAgMBAAE=
-----END PUBLIC KEY-----
```

### 3) Descifrar ubicación:

Luego coloque el archivo .dat con la ubicación en Cyber chef y me dedique a descifrarlo. En clases vimos sistemas criptográficos asimétricos, uno de ellos era RSA, así que utilice la función RSA decrypt y le coloque la llave privada.

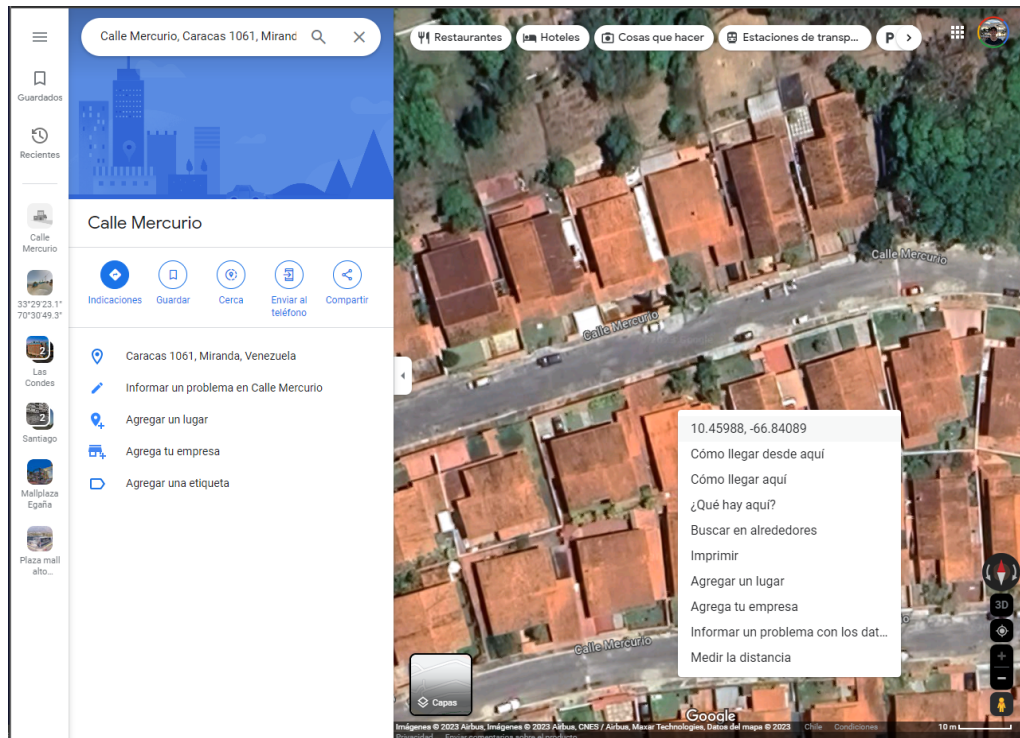
The screenshot shows the CyberChef interface. On the left, the 'Operations' list includes 'RSA Decrypt'. The 'Recipe' panel shows 'RSA Decrypt' selected, with a 'Key Password' field and 'Encryption Scheme' set to 'RSA-OAEP' and 'Message Digest Algorithm' set to 'SHA-1'. The 'Input' panel shows a file named 'CTF01-coordenadas -iniciales.dat' with a size of 128 bytes. The 'Output' panel displays the decrypted coordinates: '-33.489742, -70.513682'.

Al buscar estas coordenadas en google maps podemos ver que el premio se entregará en el edificio D de la Universidad Adolfo Ibáñez.

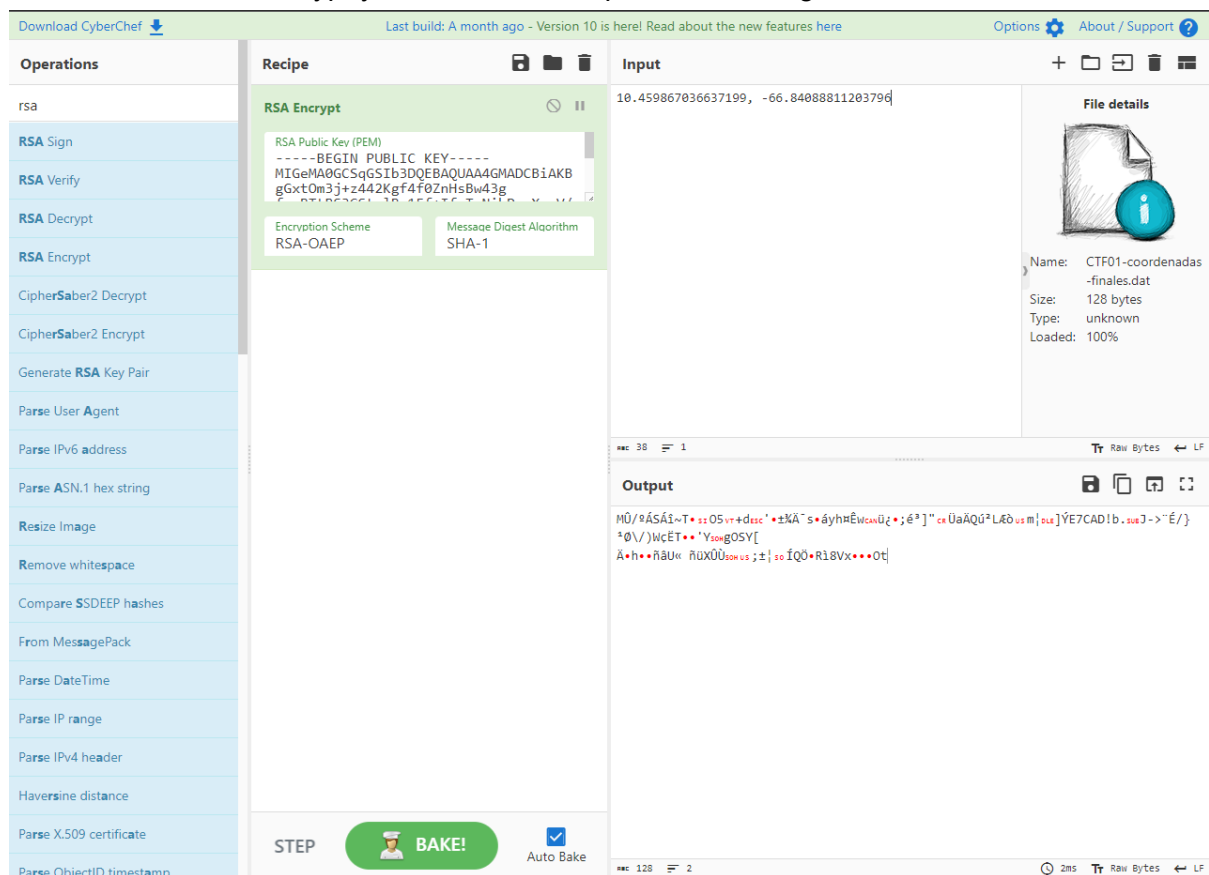


#### 4) Encriptar nueva ubicación:





Pero como bien se nos indicó, tenemos que cambiar la ubicación. Por lo cual primero busque las coordenadas de la ubicación nueva deseada:



Y después de esto, se procedió a cifrar estas nuevas coordenadas con el mismo RSA, pero esta vez la función encrypt y se utilizó la llave pública de la siguiente manera:



Para finalizar esta nueva ubicación cifrada se guarda en un archivo .dat .

 CTF01-coordenadas-finales.dat		8/25/2023 1:27 AM	DAT File	1 KB
 CTF01-coordenadas-iniciales.dat		8/25/2023 12:07 AM	DAT File	1 KB