FACULTAD DE INGENIERÍA Y CIENCIAS | UNIVERSIDAD ADOLFO IBÁÑEZ

CTF 1 – CRIPTOGRAFÍA

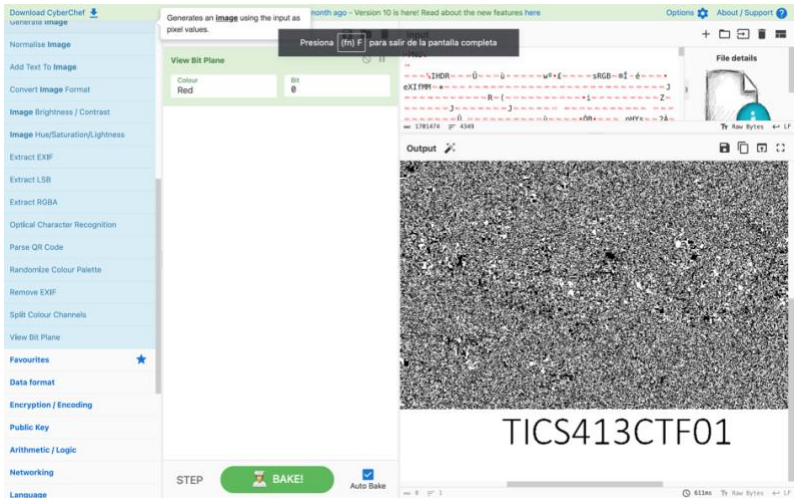
Ramo: Seguridad en TI
Profesor: Nicolás Cenzano
Alumna: Esthefany Urbano

La misión en esta ocasión se divide en dos partes. La primera parte está enfocada en encontrar las llaves, pública y privada con las que se podrá descifrar la ubicación ya no tan secreta donde se realizaría la entrega del premio en efectivo al ganador del juego 'Gran Premio'. Para luego, en la segunda parte, con las mismas llaves encontradas anteriormente, encriptar la nueva ubicación súper secreta.

1° Parte – Desencriptar

Lo primero que se hizo fue descargar la imagen enviada de manera no segura entre los funcionarios del casino, imagen que se presenta a continuación:

Posteriormente, siguiendo la recomendación de utilizar CyberChef, la imagen se colocó como Input en el software y lo que siguió de aquí fue lo más largo. Se buscaba la opción dentro de 'Operations' que fuera capaz de reconocer alguna clase de mensaje encriptado dentro de la imagen. Esta clave era vital para permitir el acceso a las llaves.
Luego de probar suficientes alternativas, se llegó a un conjunto de opciones relacionadas con 'Imágenes". Cada una fue probada. Finalmente, el último comando, 'View Bit Plane', lo logró, distorsionó por completo la imagen dejando en evidencia el mensaje que se buscaba, "TICS413CTF01". Tal como se muestra a continuación:

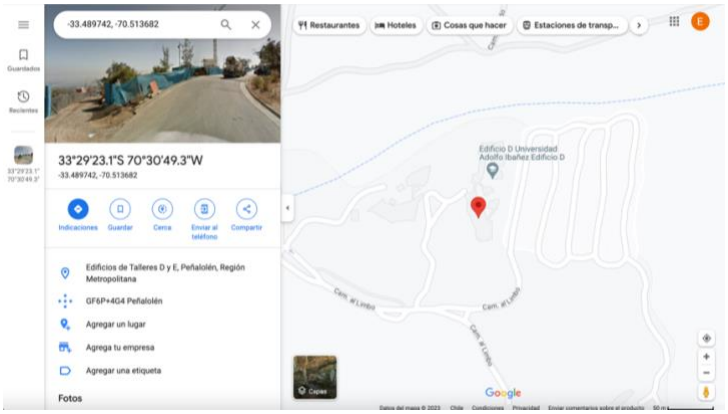


Luego, con la clave encontrada se pudo abrir el archivo ‘Llaves RSA – con contraseña’, el cual me entregó las llaves, privada y pública, que necesitaba para poder descifrar el mensaje con la ubicación no secreta. Las llaves se muestran en la siguiente imagen:

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

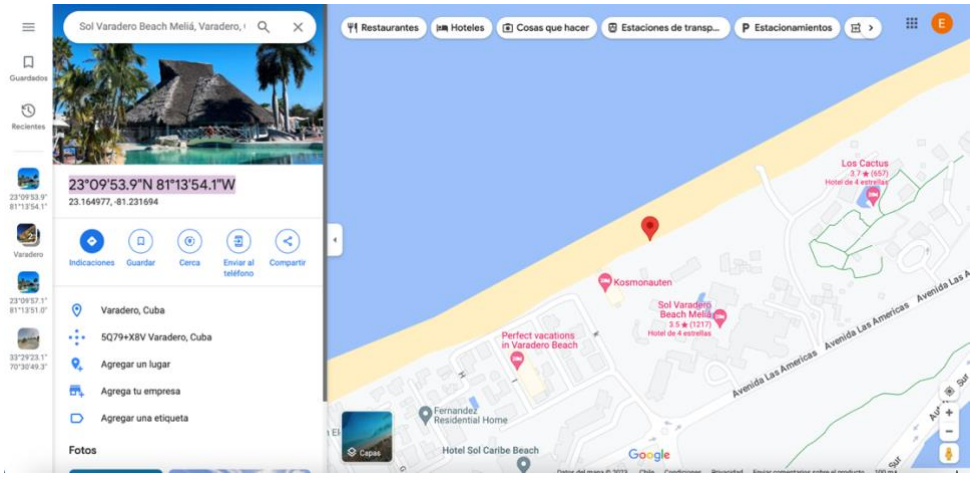
Finalmente, para encontrar las coordenadas de la primera ubicación, regresamos a CyberChef, se colocó como Input el archivo ‘CTF01-coordenadas-iniciales.dat’ y debido a que era un cifrado asimétrico, al usar una llave pública y privada, se tenía que usar un algoritmo asimétrico, el más popular es RSA, como bien se aprendió en clase. Por esto, se utilizó la operación ‘RSA Decrypt’ y con la llave privada ya encontrada, resultó en una coordenada ‘-33.48972, -70.513682’.

Esta coordenada se buscó por Google y resultó ser que la entrega del premio se iba a realizar en los edificios de talleres D y E de la Universidad Adolfo Ibáñez. Y con esto finaliza la primera parte de la misión.

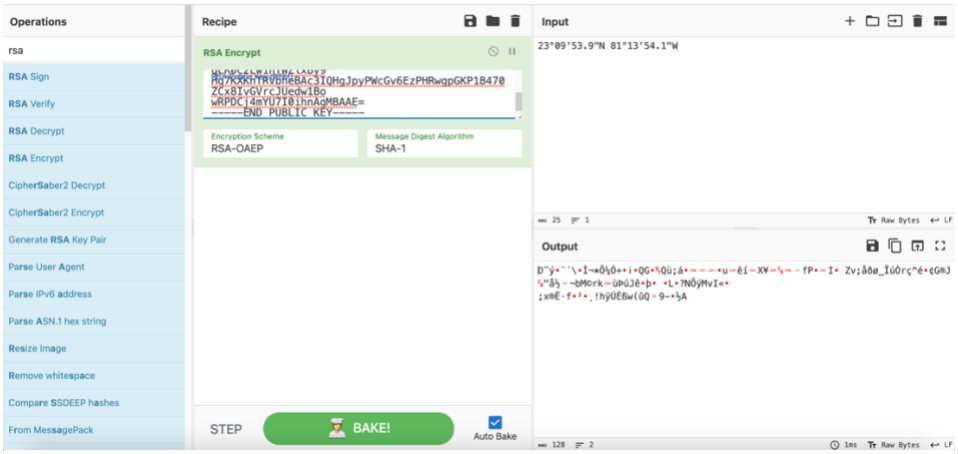


2° Parte – Encriptar

Para esta segunda parte se eligió una ubicación random en el mundo para realizar la entrega oficial del premio, en este caso una playa en Varadero, Cuba. Su ubicación exacta es ´ 23°09’53.9”N 81°13’54.1”W ´, tal como se muestra en la siguiente imagen.



Luego, se necesitaba encriptar las nuevas coordenadas. Para esto, se ingresó a CyberChef la ubicación como Input y tal como se mencionó en el enunciado se debe utilizar la misma llave pública del emisor, es decir, la llave pública que ya obtuvimos en la primera parte. Ingresando esto se logró encriptar el mensaje de manera exitosa y se procedió a guardarlo en el archivo ‘nuevas-coordenadas-Stefy.dat’.



Finalmente, se logró encriptar la nueva ubicación para la entrega del premio en efectivo con todas las especificaciones entregadas.