Resolución paso a paso de la Actividad CTF – Criptografía

Ignacio Court Palacios

Introducción

En esta actividad, se presentó el desafío de descifrar un mensaje oculto en una imagen y luego utilizar la información obtenida para abrir un pdf “protegido” que contiene llaves para descifrar coordenadas encriptadas. A continuación, se describe paso a paso cómo se abordó el desafío y las consideraciones detrás de cada paso.

Paso 1: Descargar los archivos

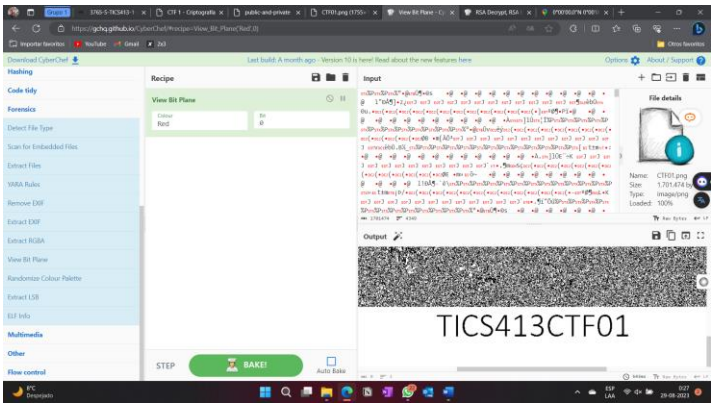
Lo primero que hice fue descargar los archivos proporcionados por el desafío: la imagen en cuestión, así como los archivos "CTF01-coordenadas-iniciales.dat" y "CTF01-keys-locked.pdf". La imagen contiene información oculta que debemos descubrir, mientras que los otros archivos podrían ser relevantes para encontrar las coordenadas de entrega de un premio de un casino.

Lo que pensé en Paso 1:

Al comienzo pensé que había que aprovechar todos los archivos para encontrar respuestas, por lo que intenté de encontrar pistas para utilizar CCrypt y desencriptar el archivo .dat o John The Ripper para poder adivinarla, sin embargo, después llegué a la conclusión (releyendo) de que debía utilizar la imagen con el software CyberChef.

Paso 2: Explorar la imagen y descubrir el mensaje oculto.

Para comenzar, cargué la imagen en la herramienta sugerida, CyberChef. Elegí esta herramienta porque es conocida por su capacidad para realizar una amplia gama de operaciones de cifrado y descifrado. Y utilicé el método "View Bit Plane" para explorar los planos de bits de la imagen. Esto reveló un código aparentemente oculto en la imagen.

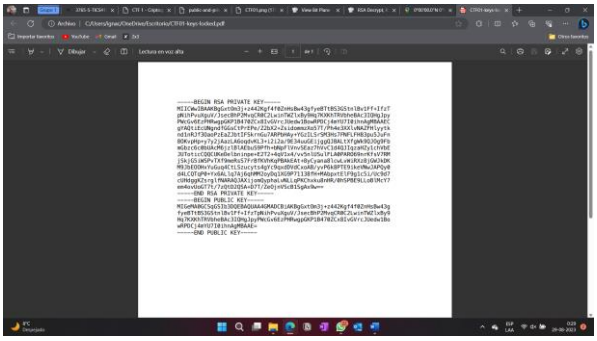


Lo que pensé en Paso 2:

Comencé a utilizar todos los métodos de Multimedia ya que pensé que eran los únicos que servían para imágenes, ninguno me estaba sirviendo, por lo que investigue sobre algunos métodos y logré entender que algunos métodos no funcionaban porque no entendían el tipo de archivo como png, porque no veían su profundidad y pensaban que era de 1 plano, y para eso existen métodos como Magic, y comencé a mezclar métodos, luego de bastante rato comencé a probar con más métodos y de repente probé View Bit Plane y mostro altiro un output, a sique revise y ahí estaba el código y supe al instante que era la contraseña del .pdf.

Paso 3: Acceso al archivo de llaves

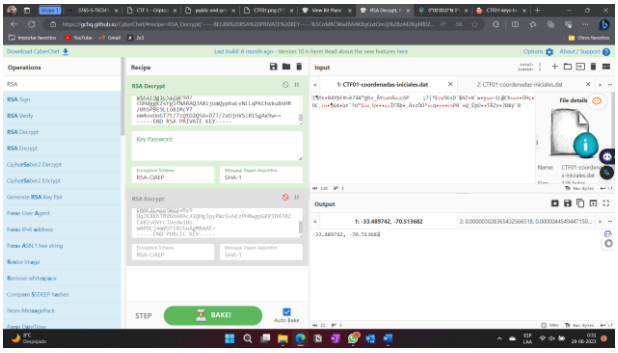
El siguiente paso fue utilizar la contraseña “TICS413CTF01” para visualizar el archivo PDF "CTF01-keys-locked.pdf". Este archivo contenía las claves pública y privada necesarias para el cifrado RSA. Esto era crucial, ya que necesitaría la clave privada para el próximo paso de descifrar las coordenadas encriptadas y posteriormente la pública para cifrar la nueva coordenada.



Paso 4: Descifrar las coordenadas

Luego de obtener la clave privada del archivo de llaves, procedí a trabajar en el archivo "CTF01-coordenadas-iniciales.dat" también desde CyberChef. Este archivo parecía contener coordenadas encriptadas. Usando CyberChef, utilicé el modo "RSA Decrypt" y proporcioné la clave privada que obtuve anteriormente para descifrar las coordenadas encriptadas.

Después de descifrar con éxito el archivo "CTF01-coordenadas-iniciales.dat", obtuve las coordenadas de ubicación del encuentro. Estas coordenadas corresponden a la ubicación donde se supone que se entregará el premio en efectivo y es la coordenada “-33.489742, -70.513682”.

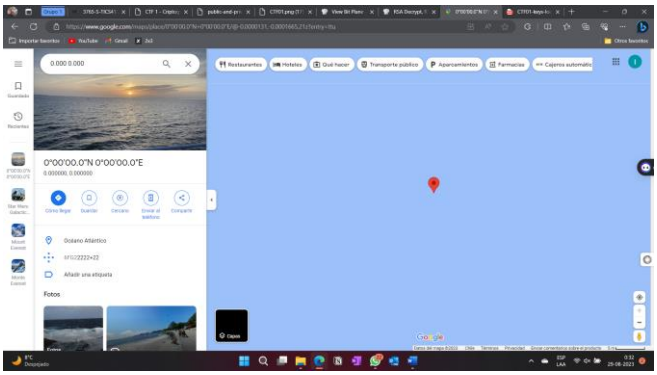


Lo que pensé en el paso 4:

Teniendo las llaves pensé en métodos para descifrar con RSA y pensé en seguir el consejo de utilizar CyberChef, apenas busqué el método apareció altiro a sique supe que solo debía usarse CyberChef, y funcionó todo a la primera.

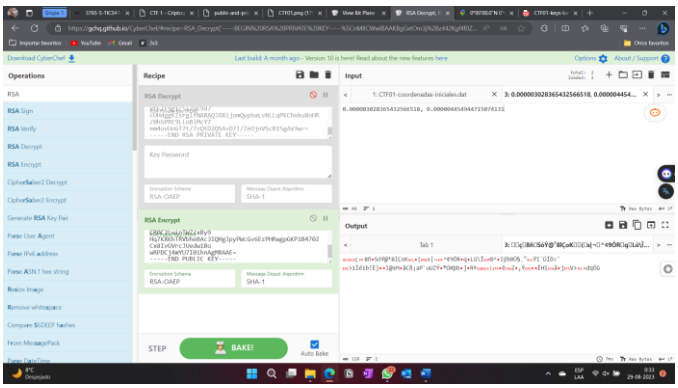
Paso 5: Sustituir las coordenadas

Accedí a Google Maps y busqué las coordenadas (0.0000, 0.0000) para obtener una ubicación inicial. Luego, copié las coordenadas reales que Google Maps me proporcionó (“0.000003028365432566518, 0.000004454944715074131”).



Paso 6: Cifrar las nuevas coordenadas

Utilicé CyberChef nuevamente, pero esta vez seleccioné el modo "RSA Encrypt". Pegué las nuevas coordenadas en el cuadro de input y proporcioné la clave pública obtenida del archivo de llaves. Luego descargué el output en un archivo .dat entregándole el nombre "CTF01-coordenadas-iniciales.dat", el cuál decidí darle ese nombre debido a que como se están sustituyendo las coordenadas de los premios del casino, no quería que los funcionarios notaran que el archivo fue modificado.



Conclusión

En este proceso, pude descubrir un mensaje oculto en una imagen, descifrar un archivo de claves protegido y obtener coordenadas encriptadas. Luego, utilicé estas llaves para generar un nuevo mensaje encriptado que reemplazó el original. Esta actividad resalta la importancia de la criptografía en la seguridad de la información y cómo los elementos ocultos en los archivos pueden llevar a soluciones ingeniosas.