

CTF1 PASOS A SEGUIR:

0) Descargar todos los archivos necesarios:

Es decir: la imagen, el pdf y las coordenadas en archivo .dat desde <https://linktr.ee/ticsuai>

1) Obtener el código de la imagen:

1.1) Utilizando la herramienta sugerida (CyberChef) cargamos la imagen como input, puesto que sabemos de antemano por el enunciado que es muy probable que haya alguna información oculta dentro de ésta que nos ayude con el trabajo:

The screenshot shows the CyberChef web application. The interface is divided into several sections:

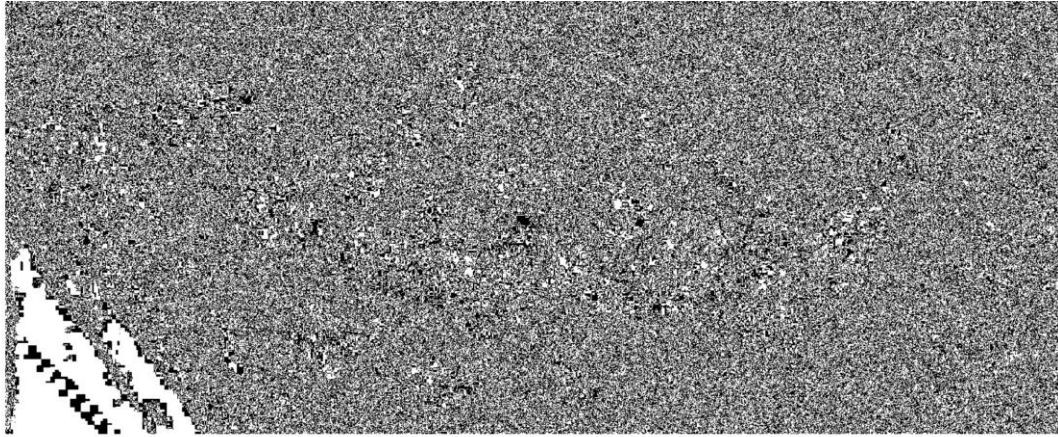
- Operations:** A sidebar on the left containing various operations like 'To Base64', 'From Base64', 'To Hex', 'From Hex', 'To Hexdump', 'From Hexdump', 'URL Decode', 'Regular expression', 'Entropy', 'Fork', and 'Magic'. It also has sections for 'Data format', 'Encryption / Encoding', 'Public Key', 'Arithmetic / Logic', and 'Networking'.
- Recipe:** A central area with a 'Recipe' tab and a 'BAKE!' button. It also has an 'Auto Bake' checkbox.
- Input:** A tab where a file named 'CTF01.png' is loaded. The file details show a size of 1,701,474 bytes and a type of 'image/png'. The 'Input' section displays the raw bytes of the file in a hex dump format.
- Output:** A tab showing the result of the operation, which in this case is the raw bytes of the input file.

1.2) Ahora debemos seleccionar la operación adecuada que nos permita obtener alguna nueva información, CyberChef nos permite buscar operaciones específicas mediante la función “Search” por lo cual buscamos alguna que sea aplicable a imágenes (buscar image).

The screenshot shows the CyberChef web application. On the left, the 'Operations' sidebar has 'Image Filter' selected. The main workspace shows a recipe with one step: 'Input' (PNG CR). Below this, a large block of hex code represents the image data. To the right, the 'File details' panel shows the file name 'CTF01.png', size '1,701,474 bytes', type 'image/png', and 'Loaded: 100%'. The 'Output' section at the bottom shows the resulting image data.

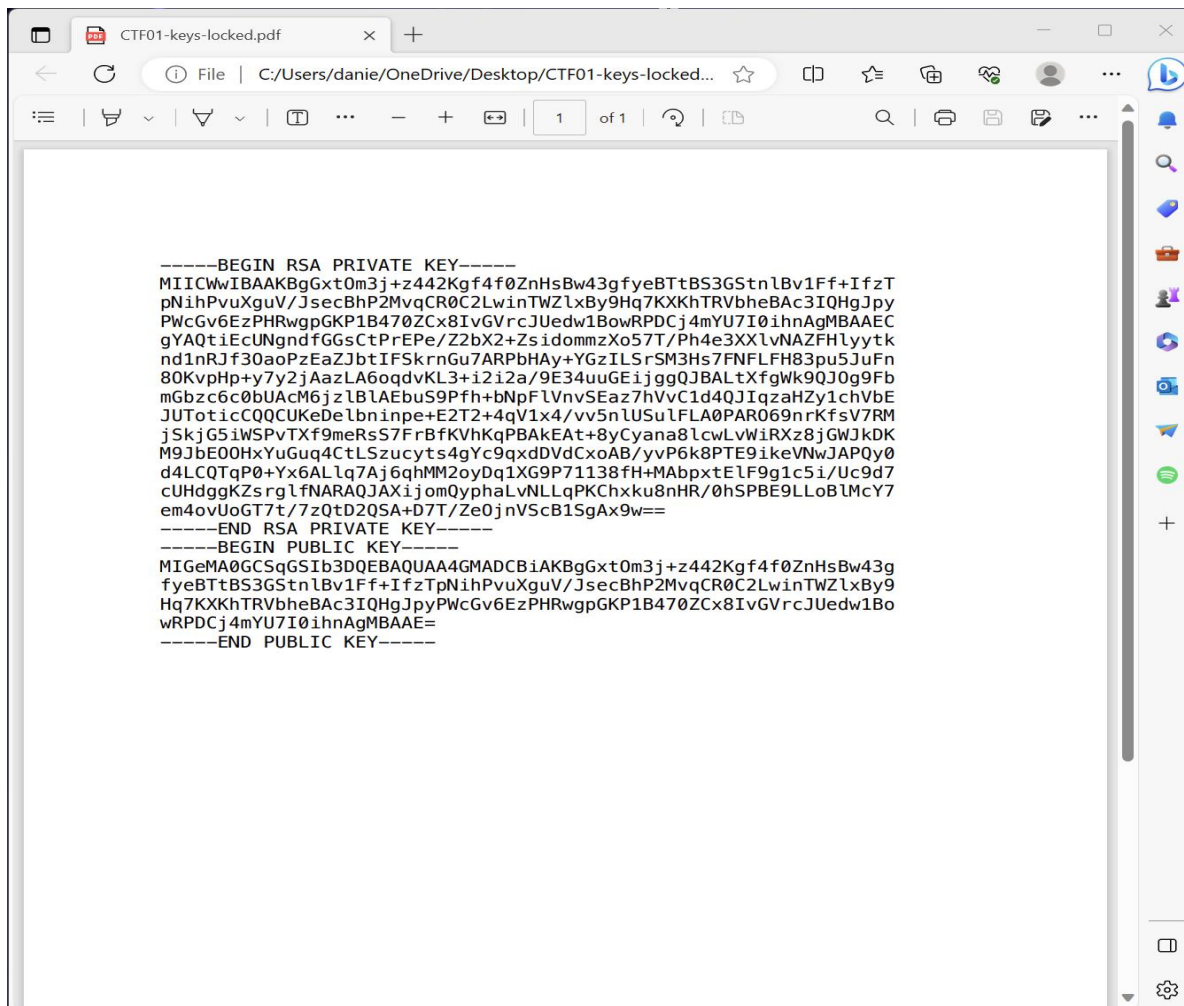
1.3) Si bien no se encontró una forma de descubrir instantáneamente cual función es la que se debe aplicar se puede ir probando una a una las posibles operaciones, incluso pasando por alto algunas que por lógica no nos entregará nueva información (recortar imagen, agregar texto, rotar, cambiar tamaño, etc.). Particularmente se llega a una operación llamada “View Bit Plane” al final de la lista, la cual entrega la siguiente información:

The screenshot shows the CyberChef web application with the 'View Bit Plane' operation selected in the left sidebar. The main workspace shows a recipe with one step: 'Input' (PNG CR). Below this, a large block of hex code represents the image data. To the right, the 'File details' panel shows the file name 'CTF01.png', size '1,701,474 bytes', type 'image/png', and 'Loaded: 100%'. The 'Output' section at the bottom shows the resulting image data, which appears as a noisy, pixelated pattern.



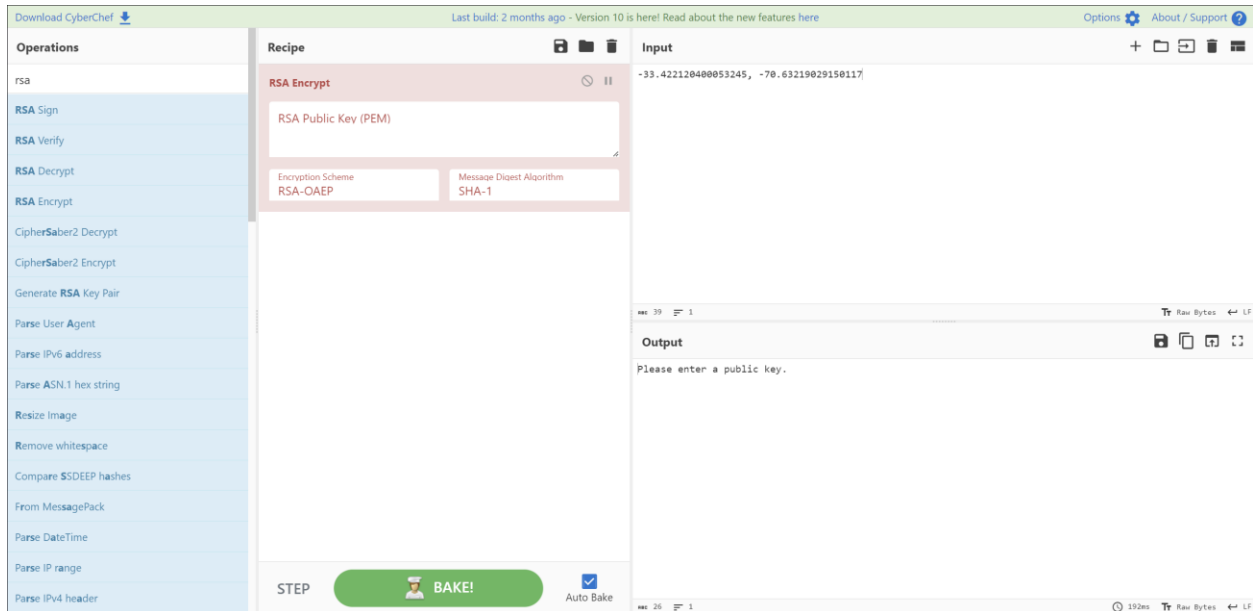
TICS413CTF01

1.4) Ahora probamos el código encontrado (TICS413CTF01) como contraseña para el archivo pdf del CTF, lo que nos permite entrar sin complicaciones

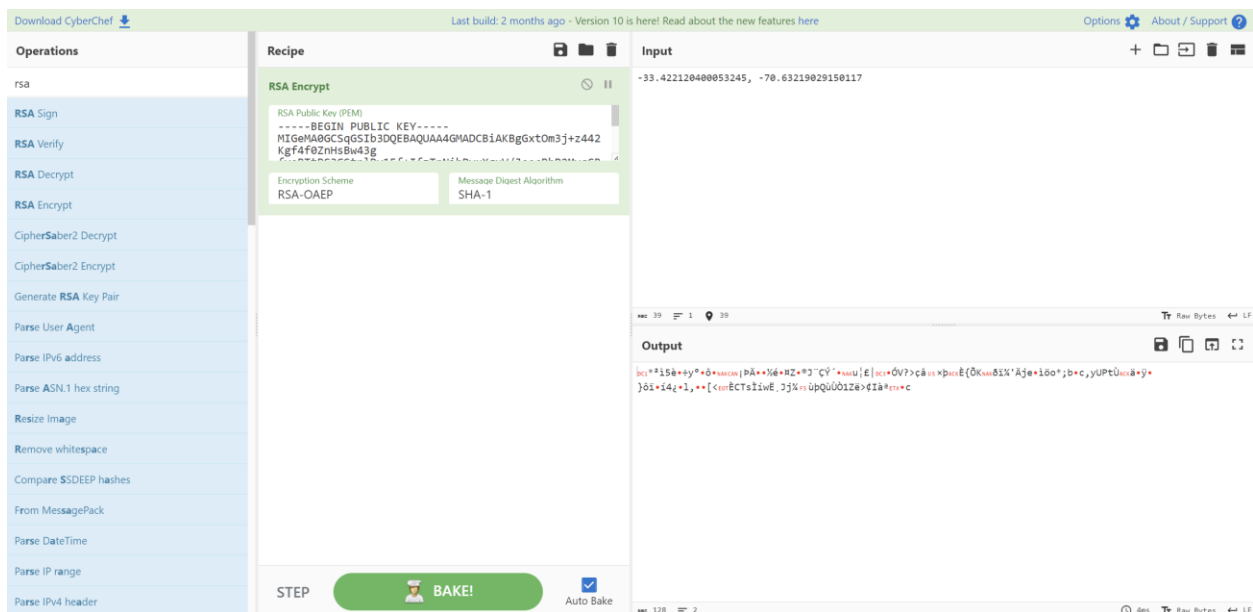


2.-) Cifrar la nueva dirección (-33.422120400053245, -70.63219029150117)

2.1) Observando la llave privada y pública del archivo nos podemos dar cuenta que se menciona RSA, utilizando CyberChef podemos cifrar y descifrar en RSA fácilmente por lo que seleccionamos esta operación utilizando como input la nueva dirección deseada:

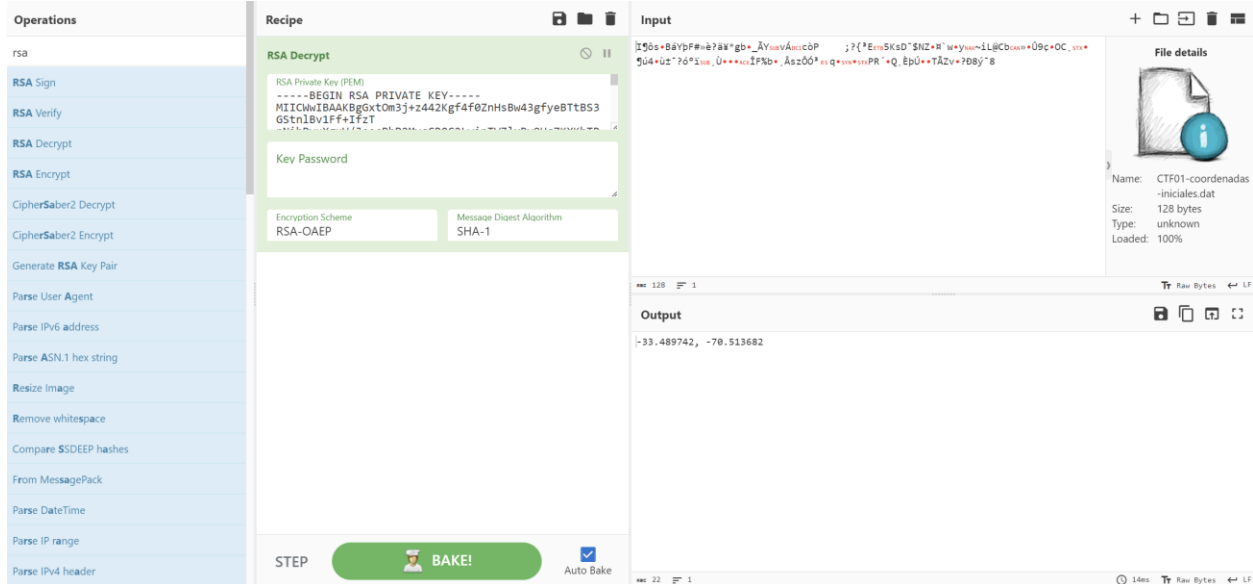


2.2) En el campo de llave publica copiamos y pegamos la que se nos entrega en el pdf, y mantenemos los otros campos como tal, resultando finalmente en un output que procedemos a guardar en un archivo .dat como CTF_Nueva_Coordenada.dat



3.) Verificar las coordenadas (opcional)

3.1) Utilizando “RSA Decrypt” procedemos a verificar que todo funciona, primero con las coordenadas iniciales rellenando el campo de llave privada con la clave que se encuentra en el pdf y utilizando como input el archivo .dat descargado desde <https://linktr.ee/ticsuai>



3.2) Nuevamente usamos “RSA Decrypt” con la misma configuración, pero ahora usando como input el archivo .dat con las coordenadas cifradas en el paso 2.

