Universidad Adolfo Ibáñez
Sede: Santiago
Seguridad en TI
Sección: 1

CTF 1
Criptografía

Profesor:
Nicolás Cenzano

Estudiante:
Vicente Garay

CTF 1 – Criptografía

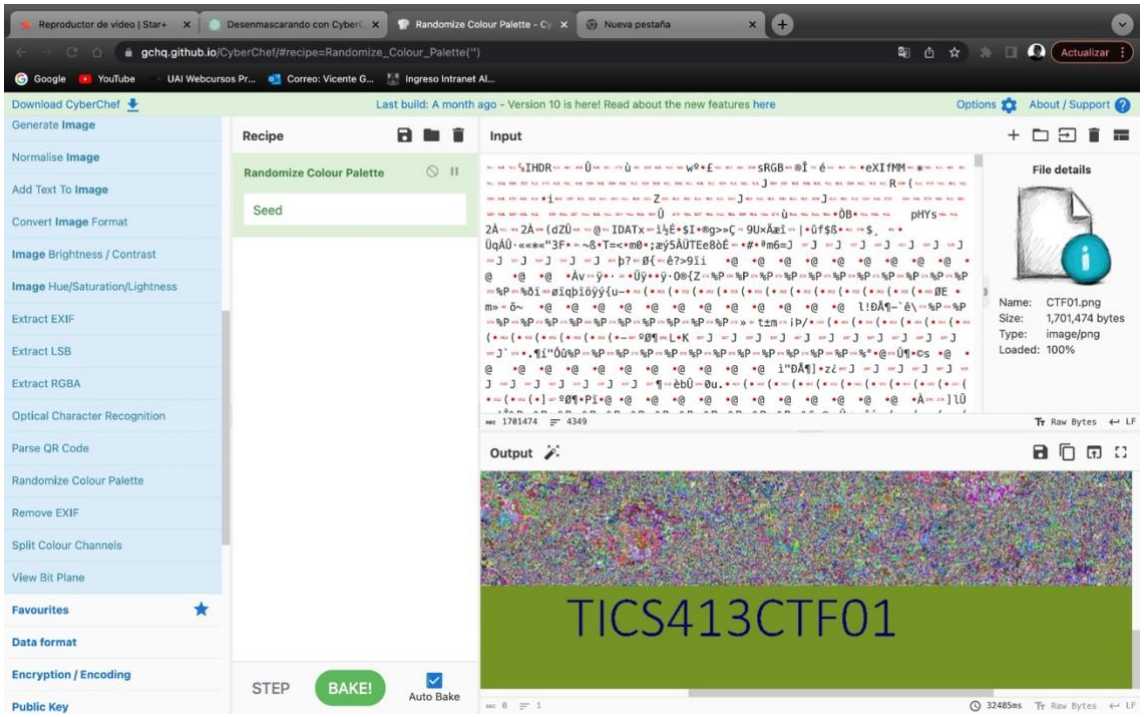
Para solucionar el CTF 1 (Capture The Flag) se llevaron a cabo los siguientes pasos:

1. Se procedió a descargar la imagen que poseía en su contenido la contraseña para acceder al documento .pdf con las llaves.
2. Se accedió a la página web de CyberChef, la cual dispone de diversas herramientas de manipulación y transformación de datos, los cual nos resulta útil, debido a que nuestro objetivo es manipular la imagen con el fin de ver el mensaje oculto.
3. Como se sabía que el archivo a manipular y transformar era uno con extensión .png, es decir, una imagen, se subió esta a la parte de "input" que nos ofrece CyberChef y en la barra de búsqueda se escribió "image" lo que nos proporcionó una serie de diversas herramientas que nos podían ser de utilidad.
4. Con la visualización de las diversas herramientas que nos ofrecía CyberChef, como: "Blur Image", "Invert Image", "Image Opacity", "Image Brightness/Contrass", "Image Hue/Saturation", "Randomize Colour Palette", entre otras muchas más, se procedió a probar una por una con la imagen para ver qué resultados arrojaba.
5. Luego de probar cada una de las herramientas, con "Randomize Colour Palette" se obtuvo el resultado deseado, ya que se consiguió visualizar en la parte de "output" el mensaje oculto en la imagen. El mensaje revelado era "TICS413CTF01".
6. Una vez obtenido este mensaje, se procedió a introducirlo en el documento .pdf que tenía contraseña de acceso, lo cual resulto exitoso, debido a que se logró efectivamente acceder al contenido de este.
7. Una vez visualizada la información del documento .pdf, que eran las llaves públicas y privadas con las que se habían cifrado las coordenadas de entrega del premio, se procedió nuevamente a hacer uso de la herramienta de CyberChef.
8. Esta vez CyberChef iba a ser utilizado para las tareas de desencriptación y encriptación, debido a que queremos ver cuáles son las coordenadas iniciales, de modo que se pueda saber cuáles son y no repetirlas por accidente y del mismo modo, probar si las llaves funcionan correctamente.

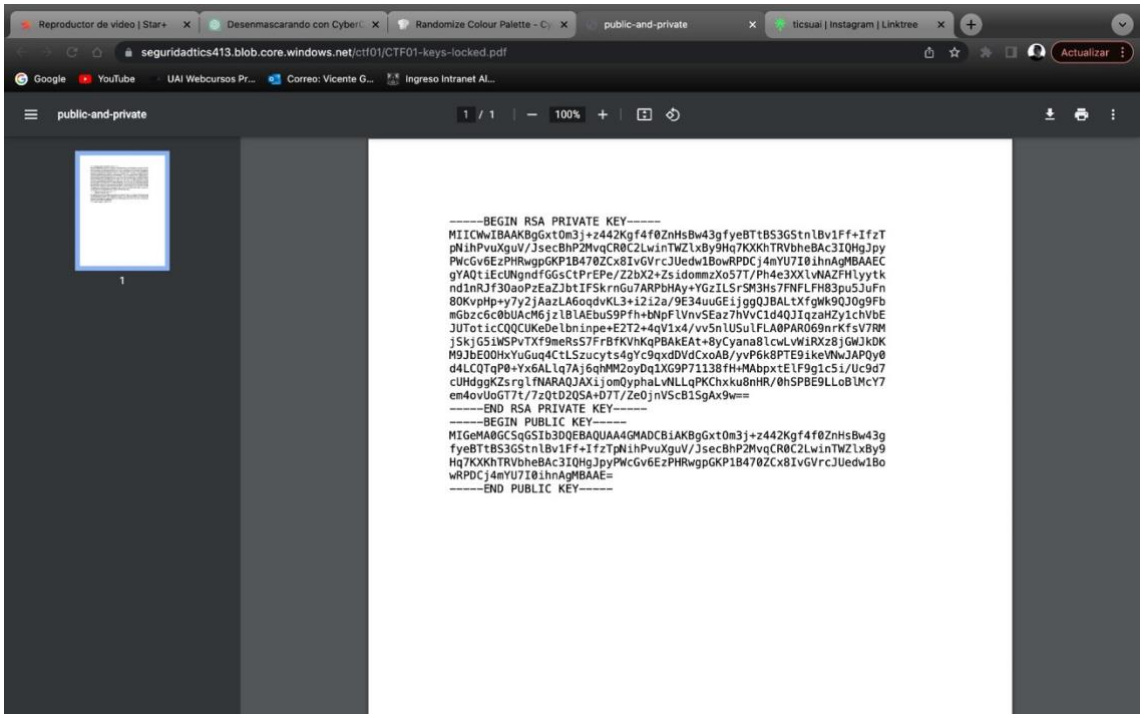
9. Al observar que las llaves obedecían a un formato RSA (Rivest-Shamir-Adleman) se procedió a escribir “RSA” en el buscador de CyberChef, apareciendo las herramientas de “RSA Encrypt” y “RSA Decrypt”.
10. Para ver las coordenadas iniciales, se subió a la parte de “input” el archivo con extensión .dat, y luego se seleccionó la herramienta “RSA Decrypt”, donde nos pedía la llave privada para poder desencriptar la información, por ende, se colocó la llave privada que estaba en el .pdf y en la parte de “output” arrojo que eran “-33.489742, -70.513682” las cuales al introducirlas en “Google Maps” nos daba como ubicación los edificios de Talleres D y E de la Universidad Adolfo Ibáñez.
11. Una vez vista la ubicación inicial y que las llaves funcionaban correctamente, se procedió a escoger la nueva ubicación, introducirla en la parte de “input” de CyberChef y seleccionar la herramienta “RSA Encrypt”, donde se solicitó la llave publica para realizar el cifrado, donde se colocó la llave publica que estaba en el documento .pdf y en la parte de “output” se obtuvieron las nuevas coordenadas cifradas, y dándole al botón de descargar se consiguió un nuevo archivo .dat con las información cifrada.

Anexos

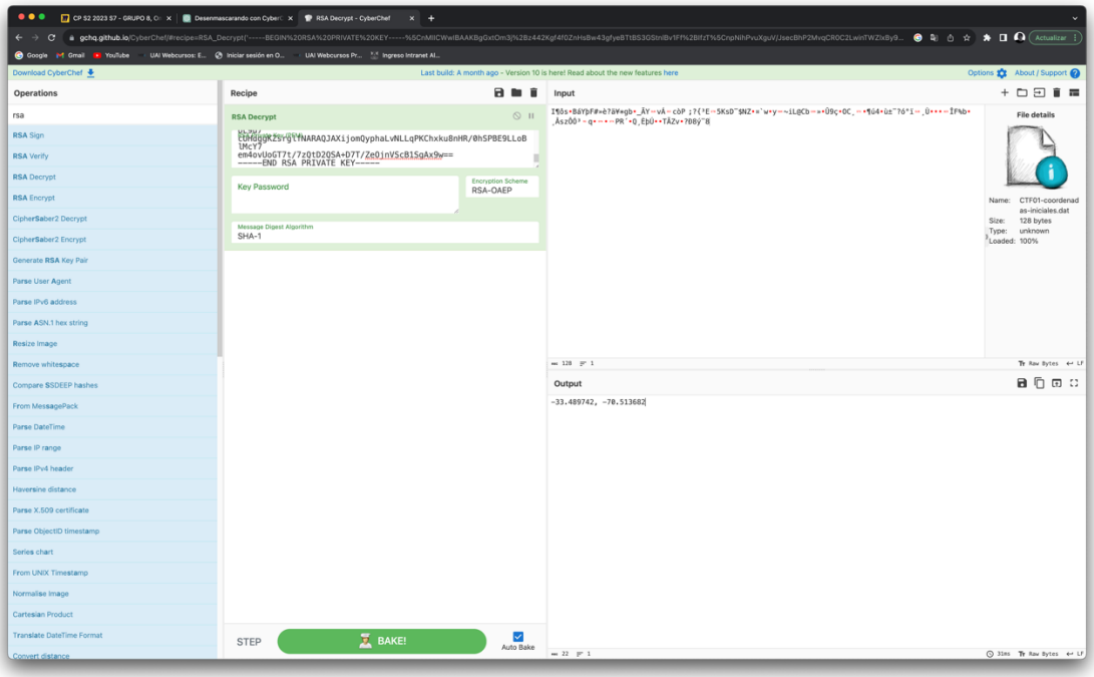
1. Imagen donde se visualiza la obtención del mensaje oculto en el archivo .png



2. Información dispuesta en el archivo .pdf que poseía clave



3. Desencriptación de las coordenadas iniciales



4. Visualización de las coordenadas iniciales en Google Maps