

CTF01 – Agustín Brito Cejas

En primer lugar se obtendrá la contraseña del pdf que contiene las llaves pública y privada. Para ello, como se menciona en las instrucciones se utilizará la imagen entregada. Antes de implementar alguna herramienta, se revisó minuciosamente la imagen, esto para intentar apreciar patrones o códigos escondidos, pero al no encontrarlos a simple vista, se acudió a la herramienta recomendada Cyberchef. Se probaron algunas funciones para cambiar los filtros y colores de la imagen, como Image filter, opacity, hue / saturation / lightness, etc. Pero ninguna entregó códigos visibles. Luego de probar con distintas funciones se encontró que, usando la función randomize colour palette, la imagen arrojaba un código oculto (TICS413CTF01). Dicha función ayuda a visibilizar códigos o textos ocultos debido a la similitud entre este y el fondo de la imagen (el marco negro), cosa que a simple vista no era apreciable. Dicho código abre el pdf mencionado anteriormente con las llaves.

Una vez obtenida las llaves, se utilizó la función de cyberchef RSA Decrypt, ya que en el archivo de llaves se aprecia el nombre de dicho algoritmo por lo que se intentó con dicho método, entregando como input el archivo .dat de las coordenadas iniciales. Dicha función necesitará de la llave privada encontrada anteriormente, obteniéndose las coordenadas -33.489742, -70.513682, las cuales pertenecen a la dirección de la universidad Adolfo Ibáñez.

Sabiendo donde se entregará el premio, ahora se buscará enviarlos a otra ubicación. Para ello se utilizará la ubicación de Epcot. De esta forma, siguiendo la misma idea anterior, se implementó RSA para encriptar las coordenadas del nuevo lugar (28.377635955800244, -81.54919214290851), entregando como input dichas coordenada y como receta la función de Cyberchef RSA Encrypt, la cual requiere de la llave pública encontrada previamente, obteniéndose así un nuevo archivo .dat con la ubicación encriptada.