Paso a Paso CTF 01

1. Primero descargué la imagen y la subí como Input a CyberChef para empezar a probar las distintas funciones para encontrar la clave oculta.

2. Fui al apartado de Forensics y usé la función llamada “Randomize Colour Palette”. Usé esa porque esta podía revelar texto que fuese del mismo color de alguna sección de la imagen, y dado que la clave estaba oculta en el borde, la herramienta funcionó perfectamente. La clave oculta era:

   TICS413CTF01

3. Posteriormente usé la clave “TICS413CTF01” para abrir el pdf “CTF01-keys-locked.pdf” que contenía la clave pública y privada. Estas eran:

   -----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-----

4. Subí el archivo “CTF01-coordenadas-iniciales.dat” a CyberChef para desencriptarlo y saber qué función se utilizó. Esto para conocer que herramienta usar para encriptar las nuevas coordenadas.

5. En Recipe puse la función “RSA Decrypt” y la clave privada para desencriptarlo. Las coordenadas originales eran:

   -33.489742, -70.513682

6. Finalmente quedaba encriptar un nuevo mensaje con otras coordenadas. Escogí las siguientes: 51.496845, -115.928055
   Corresponden a un Parque Nacional en Canadá, llamado Banff.

7. Por último, como Input ingresé esas nuevas coordenadas. Usé la función “RSA Encrypt” y la clave pública para encriptarlo. El archivo de salida encriptado es “smaCTF01.dat”.