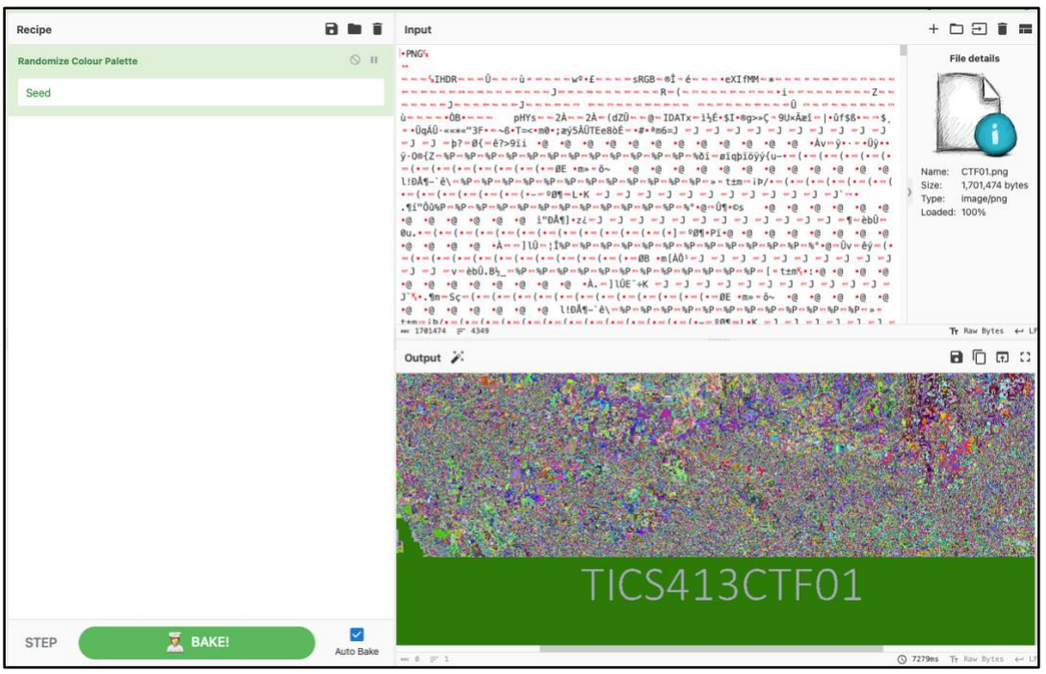
Seguridad TI - TICS413

Capture The Flag - CTF

José de la Barra Cortés
jodelabarra@alumnos.uai.cl

Paso 1: Dado que el código que sirve para acceder al PDF se encontraba en una imagen, en primer lugar, busqué “image” en el buscador de herramientas de Cyberchef y fui probando cada una de las herramientas.
Cuando probé la herramienta “Randomize Colour Palette”, percaté que en la franja negra inferior de la imagen aparecieron unas letras que antes se encontraban ocultas.



Paso 2: Probé acceder exitosamente al PDF con la contraseña “TICS413CTF01”
En la siguiente imagen se muestra lo que contenía dicho PDF.

```
-----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-----
```

Paso 3: Como se puede observar, el inicio y término de la clave privada sugieren que las coordenadas se encriptaron usando RSA. Es por esto que busqué “RSA decrypy” en las herramientas de Cyberchef.

Paso 4: Usé la herramienta “RSA decrypy” llenando los siguientes campos:

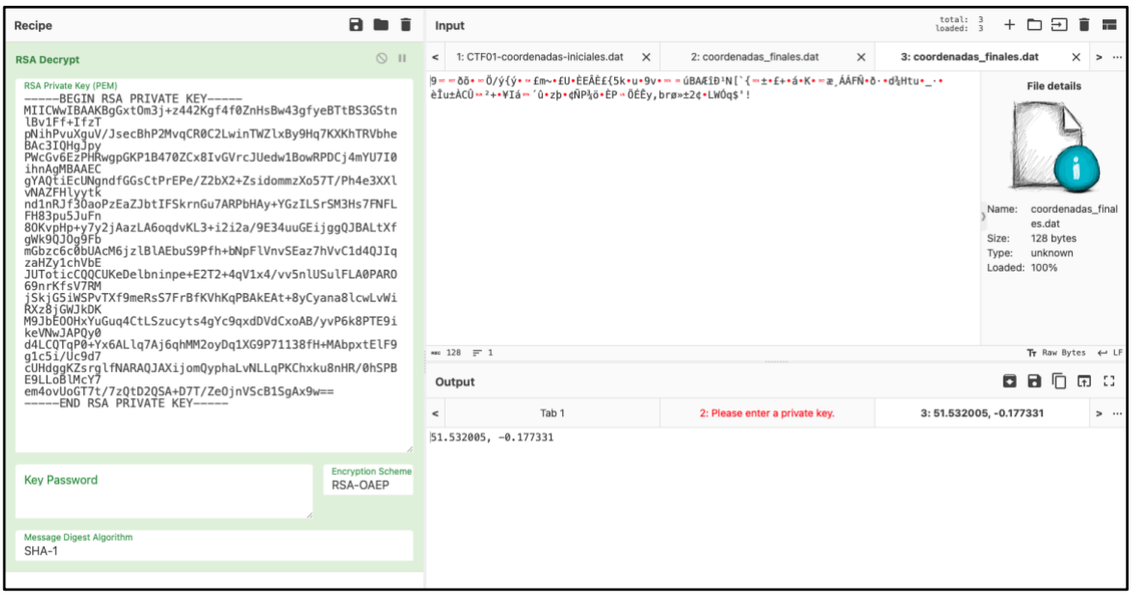
RSA Private Key (PEM): con la clave privada conseguida en el PDF protegido.
Input: con las coordenadas iniciales encriptadas.

Todo lo demás lo dejé por default.

Como se observa en la imagen, resultado del paso anterior se consiguieron las coordenadas que se encontraban encriptadas. Estas coordenadas son -33.489742, -70.513682 y corresponden a la entrada del estacionamiento del edificio D de la UAI (Campus Peñalolen).

Paso 5: Escogí nuevas coordenadas y las encripté realizando el proceso inverso, es decir, utilizando la herramienta “RSA Encrypt” y la llave pública contenida en el archivo PDF.

Paso 6: Con tal de probar la correspondencia entre la llave pública y la llave privada, ingresé el output de la operación anterior a la herramienta de desencriptado de RSA y ocupé la misma llave privada contenida en el archivo PDF.



Se observa que el output corresponde a las mismas coordenadas elegidas en un principio por lo que, se verificó la herramienta RSA para encriptar las coordenadas con las llaves privadas y públicas dadas.