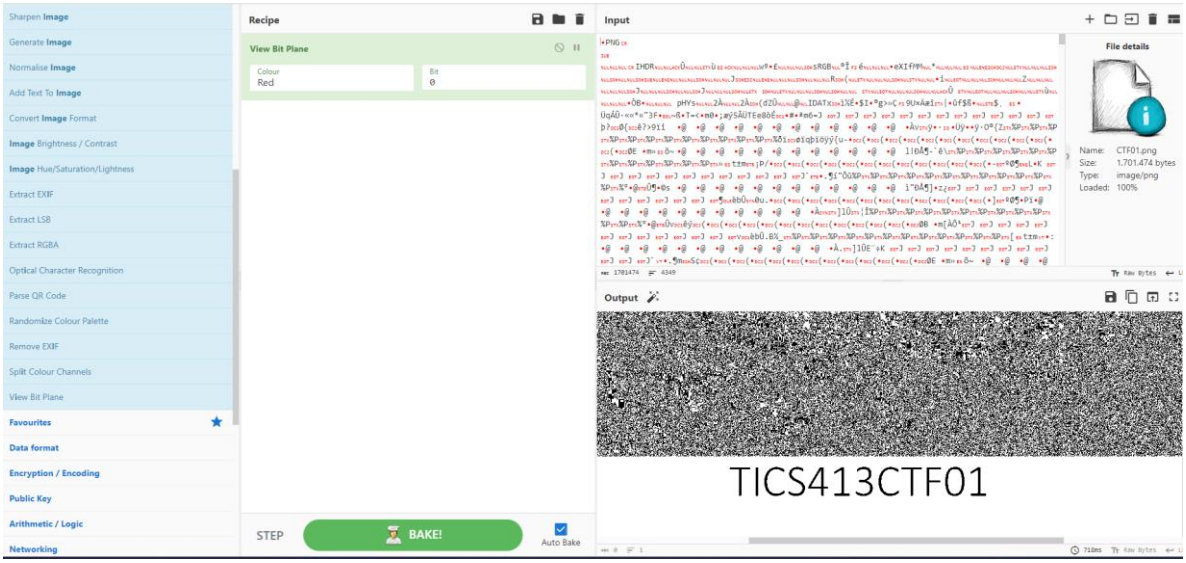
Capture The Flag 1

Klaus Molt

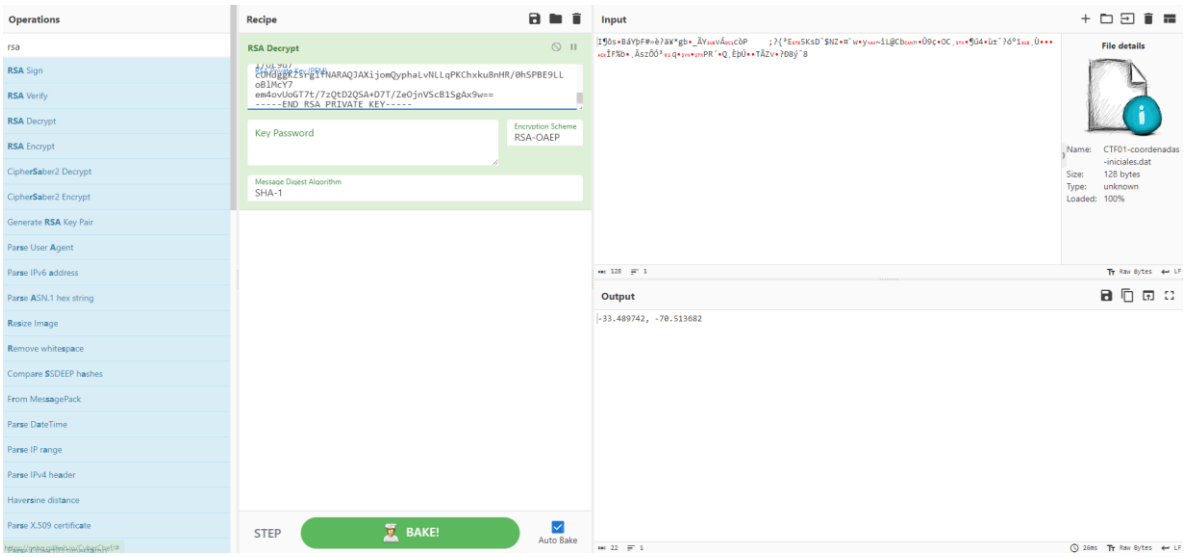
1. El primer paso es descargar los archivos que se nos entregan para hacer el Capture The Flag, estos consisten en una imagen, un PDF con contraseña y un .dat.
2. Se debe ingresar la imagen a Cyberchef. Aquí, de forma intuitiva, se entendió que, para obtener la clave, se debería hacer algún tipo de alteración de imagen. Por lo que se buscaron todas las recetas que aparecen al buscar “Image”. Mediante prueba y error, llegué a la receta View Bit Plane. Al mostrar solo un bit de cada imagen, se revela una clave en el borde negro de la foto entregada.



3. Ingresar la clave en el archivo bloqueado. En este caso, nos permitirá observar la clave privada y pública de un método RSA. Identifiqué que este era el método por haberlo recordado en clases y, además, este está escrito en las mismas claves del documento.

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z442Kgf4f0ZnHsBw43gfyeBTtBS3GStnlBv1Ff+IfzT
pNihPvuXguV/JsecBhP2MvqCR0C2LwinTWZlxBy9Hq7KXKhTRVbheBAc3IQHgJpy
PWcGv6EzPHRwgpGKP1B470ZCx8IvGVrcJUedw1BowRPDCj4mYU7I0ihnAgMBAAEC
gYAQtiEcUNgndfGGsCtPrEPe/Z2bX2+ZsidommzXo57T/Ph4e3XXlvNAZFHlyytk
nd1nRJf3OaoPzEaZJbtIFSkrnGu7ARPbHAy+YGzILSrSM3Hs7FNFLFH83pu5JuFn
8OKvpHp+y7y2jAazLA6oqdvKL3+i2i2a/9E34uuGEijggQJBALtXfgWk9QJOg9Fb
mGbzc6c0bUAcM6jzlBlAEbuS9Pfh+bNpFlVnvSEaz7hVvC1d4QJIqzaHZy1chVbE
JUTotic CQQCUKeDelbninpe+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. El siguiente paso es introducir el archivo .dat en el cyberchef. Dado a la inferencia anterior, debemos buscar una receta que nos permita desencriptar este mismo. Este corresponde a RSA Decrypt,
5. Esto permitirá poner la clave privada que nos entregará las coordenadas. Al buscarlas en Google sabemos que estas corresponden a la Universidad Adolfo Ibañez.



6. Luego se deben seleccionar coordenadas a gusto, las que servirán para enviar el nuevo archivo pedido.
7. Estas se deben decodificar utilizando el mismo método RSA. Lo que implica buscar el método de RSA Encrypt.
8. Finalmente, veremos que esa receta solicita la clave pública del documento que se abrió al principio. Lo que nos entregará la misma información cifrada que podremos descargar en su propio .dat.