

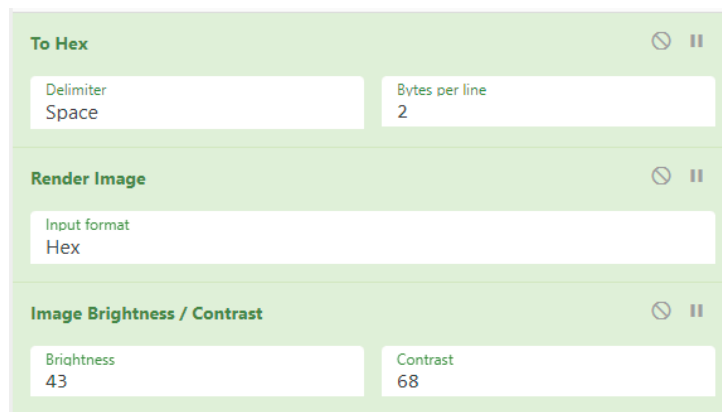
Paso a paso CTF01-TICS413

Mario Rozas

1.- Se descargan los archivos “CTF01.png”, “CTF01-keys-locked.pdf” y “CTF01-coordenadas-iniciales.dat” del siguiente link: <https://linktr.ee/ticsuai>

2.- Luego se debe abrir la imagen correspondiente. En un monitor OLED se ve a simple vista que debajo en la imagen sale el texto “TICS413CTF01”. En caso de no ser así, se debe modificar los parámetros de la imagen tales como el brillo para que se aprecie claramente esto.

En la página <https://gchq.github.io/CyberChef/> se debe de utilizar la imagen de input, para luego hacer las siguientes operaciones sobre la imagen:



The screenshot shows the CyberChef web interface with three sections:

- To Hex**: Delimiter is set to "Space", Bytes per line is set to "2".
- Render Image**: Input format is set to "Hex".
- Image Brightness / Contrast**: Brightness is set to "43", Contrast is set to "68".

Con lo que la imagen se verá de la siguiente manera:



3.- Con este código se debe ingresar al PDF con contraseña y utilizar el mismo en ese espacio, con lo cual se podrá acceder al contenido de este.

4.- Con la llave RSA pública y privada obtenidos del PDF, se puede cifrar y descifrar coordenadas. Primero se descifrará el archivo .dot en cuestión.

Para esto se debe ir a la página de CyberChef nuevamente y subir el archivo de las coordenadas iniciales como input. Luego se debe utilizar la operación “RSA Decrypt” para obtener estas coordenadas.

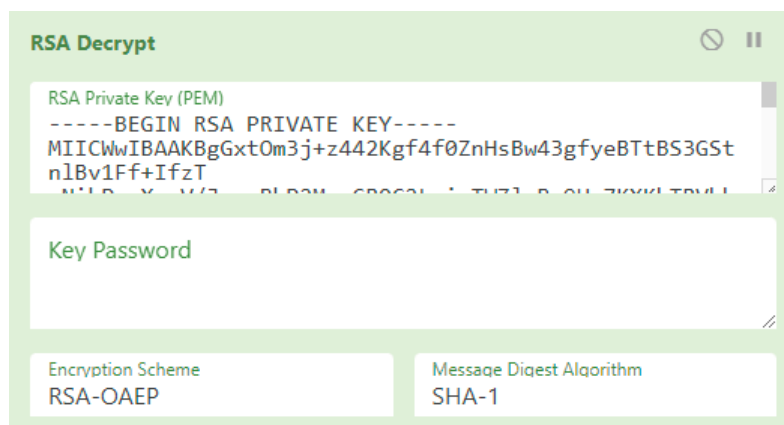
Se debe introducir la private key obtenida previamente, la cual es:

-----BEGIN RSA PRIVATE KEY-----

```
MIICWwIBAAKBgGxtOm3j+z442Kgf4f0ZnHsBw43gfyeBTtBS3GStnBv1Ff+IfzT
pNihPvuXguV/JsecBhP2MvqCR0C2LwinTWZlxBy9Hq7KXKhTRVbheBAc3IQHgJpy
PWcGv6EzPHRwgpGKP1B470ZCx8lvGVrcJUedw1BowRPDCj4mYU7I0ihnAgMBAAEC
gYAQtiEUNgndfGGsCtPrEPe/Z2bX2+ZsidommzXo57T/Ph4e3XXlvNAZFHlyytk
nd1nRjF3OaoPzEaZJbtIFSkrnGu7ARpbHAy+YGzILSrSM3Hs7FNFLFH83pu5JuFn
8OKvpHp+y7y2jAazLA6oqdvKL3+i2i2a/9E34uuGEijggQJBALtXfgWk9QJOg9Fb
mGbzc6c0bUAcM6jzIBIAEbuS9Pfh+bNpFIVnvSEaz7hVvC1d4QJlqzaHZy1chVbE
JUToticCQQCUKeDelbninpe+E2T2+4qV1x4/vv5nlUSulFLA0PARO69nrKfsV7RM
jSkjG5iWSPvTXf9meRsS7FrBfKVhKqPBAkEAt+8yCyana8lcwLvWiRXz8jGWJkDK
M9JbE0OHxYuGuq4CtLSzucyts4gYc9qxdDVdCxoAB/yvP6k8PTE9ikeVNwJAPQy0
d4LCQTqP0+Yx6ALlq7Aj6qhMM2oyDq1XG9P71138fH+MAbpxtEIF9g1c5i/Uc9d7
cUhdggKZsrglfNARAQJAXijomQyphaLvNLLqPKChxku8nHR/0hSPBE9LLOBIMcY7
em4ovUoGT7t/7zQtD2QSA+D7T/ZeOjnVScB1SgAx9w==
```

-----END RSA PRIVATE KEY-----

Debiera verse de la siguiente manera en la página:



The screenshot shows the 'RSA Decrypt' interface. The 'RSA Private Key (PEM)' field is populated with the private key text. The 'Key Password' field is empty. The 'Encryption Scheme' is set to 'RSA-OAEP' and the 'Message Digest Algorithm' is set to 'SHA-1'.

Con lo que se obtendrá el siguiente output: -33.489742, -70.513682

Correspondiendo las coordenadas iniciales donde se recibirá el premio del nuevo ganador del efectivo a la Universidad Adolfo Ibáñez, específicamente el edificio E.

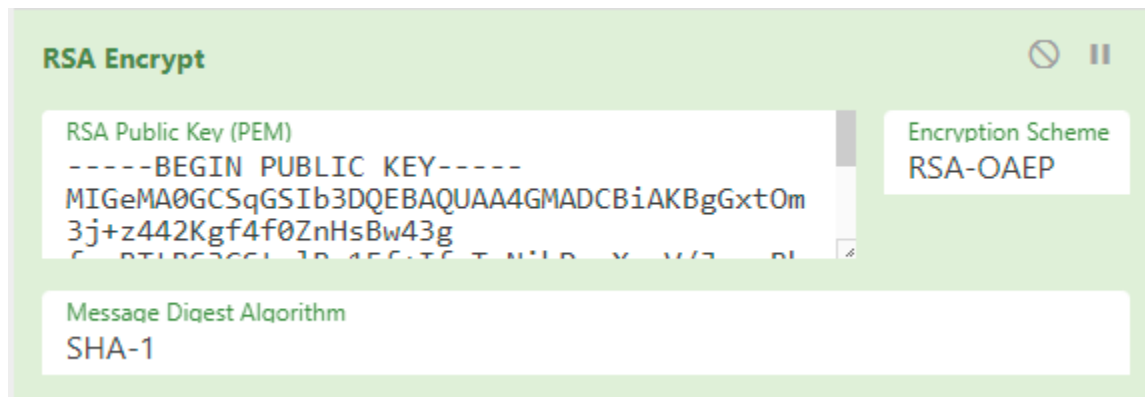
5.- Por último, para sustituir estas coordenadas por otras se debe utilizar la operación “RSA Encrypt” en la misma página, usando de public key:

-----BEGIN PUBLIC KEY-----

```
MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgGxtOm3j+z442Kgf4f0ZnHsBw43g
fyeBTtBS3GStnBv1Ff+IfzTpNihPvuXguV/JsecBhP2MvqCR0C2LwinTWZlxBy9
Hq7KXXhTRVbheBAc3IQHgJpyPWcGv6EzPHRwgpGKP1B470ZCx8lvGVrcJUedw1Bo
wRPDCj4mYU7I0ihnAgMBAAE=
```

-----END PUBLIC KEY-----

Viéndose de la siguiente manera:



El input pueden ser las nuevas coordenadas que se estimen convenientes. En este caso son: - 34.772964, -71.038139.