

---

## TICS 413 Seguridad en TI

2º Semestre 2023 | Campus Peñalolén.

---

### CTF 1 - Criptografía

- Benjamin Astrain

---

El siguiente documento contiene un informe detallado acerca del proceso de descriptación y encriptación de archivos e información para la clase de criptografía. La tarea descrita consistió en analizar tres archivos de distinto formato cada uno, para luego con la ayuda de la herramienta “Cyberchef” poder descriptar y encontrar la información oculta en estos. A continuación, se procederá a explicar el paso a paso a seguir para poder extraer la información y cumplir con la tarea asignada, así como también se dará a conocer que es y cómo se utilizó la herramienta “Cyberchef.” Es una herramienta online diseñada para ayudar a todo tipo de usuarios, con o sin experiencia en informática, a poder realizar distintos tipos de operaciones tales como encriptar, comprimir, codificar y analizar datos.

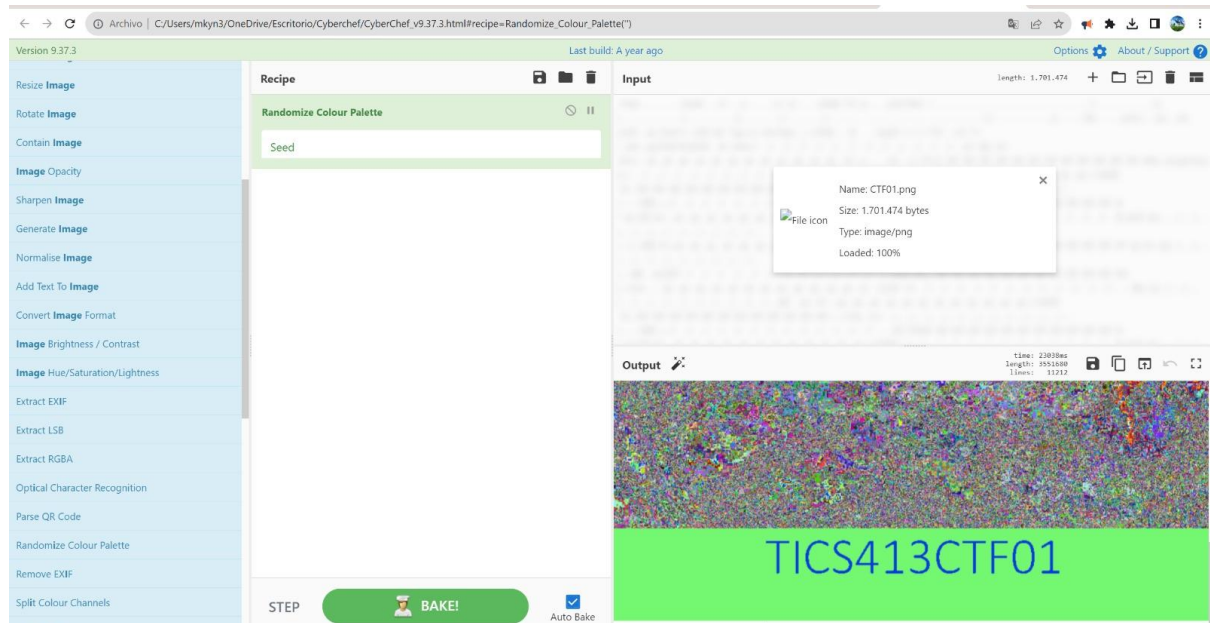
Dentro de las herramientas que ofrece la plataforma encontramos diferentes opciones para trabajar los archivos, en este caso, el primer paso fue utilizar la herramienta para encontrar información oculta en un archivo “.png” para lo que el software ofrece las opciones de: aleatorizar la paleta de colores, modificar el tamaño, contraste y orientación de la imagen, así como otras más avanzadas tales como extraer el RGBA y el reconocimiento óptico de caracteres. A continuación, se procederá a explicar cuáles fueron los archivos analizados y como se procedió con cada uno de ellos según el tipo de archivo del que se trata y de como se necesita operar con él, ya sea para extraer información o para desbloquearlo.

#### Paso 1. Archivos y procesado de datos en cyberchef

La entrega realizada a los estudiantes consistió en tres archivos, cada uno con diferente información, propósito, y formato a través de un link con la instrucción de la actividad.. Los archivos se encontraban en formatos: “.png”, “.pdf” y “.dat”. el primer archivo, el que corresponde a una imagen de la película “misión imposible”, esta imagen se cargó a la plataforma “Cyberchef” para posteriormente poder utilizar las diferentes herramientas con las que esta cuenta y así poder encontrar cualquier información oculta en la imagen.

Los resultados aparecieron una vez se escogió la opción “Randomize colour pallette” lo que traducido al español significa “Aleatorizar la paleta de colores”, de esta manera se encuentra con el primer código que puede verse en la imagen.

Ilustración 1 captura de pantalla del resultado de utilizar cyberchef en la imagen.

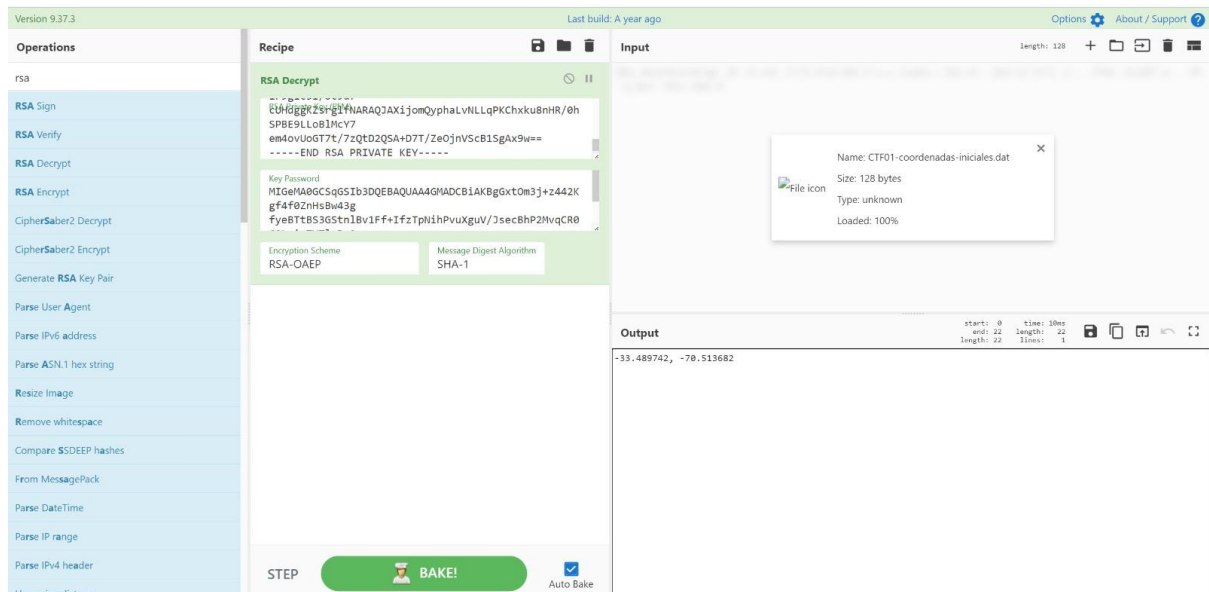


## Paso 2. Utilización y desbloqueo de archivos

Luego de conseguido el código de la ilustración 1, se procede a utilizar ese código para poder desbloquear el archivo “.pdf”, una vez desbloqueado este archivo, se comienza a analizar su contenido, en este, se puede encontrar dos tipos de llaves de descriptado: una pública y una privada de RSA.

## Paso 3. Descriptación del archivo .dat

Con la utilización de las llaves obtenidas del archivo .pdf, se volvió a utilizar la plataforma “Cyberchef”, seleccionando RSA Descript para poder utilizar las llaves y descriptar el archivo. Las llaves se utilizarán para poder ser introducidas en el archivo “.dat” cargado a la plataforma, de esta manera se obtiene acceso a los datos de este. Una vez hecho esto, se puede acceder a unas coordenadas, que dirigen hacia la Universidad Adolfo Ibáñez.



Version 9.37.3 Last build: A year ago Options About / Support

**Operations**

- rsa
- RSA Sign
- RSA Verify
- RSA Decrypt
- RSA Encrypt
- CipherSaber2 Decrypt
- CipherSaber2 Encrypt
- Generate RSA Key Pair
- Parse User Agent
- Parse IPv6 address
- Parse ASN.1 hex string
- Resize Image
- Remove whitespace
- Compare SSDEEP hashes
- From MessagePack
- Parse DateTime
- Parse IP range
- Parse IPv4 header
- Haversine distance

**Recipe**

RSA Decrypt

Input

Length: 128

File icon

Name: CTF01-coordenadas-iniciales.dat

Size: 128 bytes

Type: unknown

Loaded: 100%

Output

start: 0 time: 10ms

end: 22 length: 22

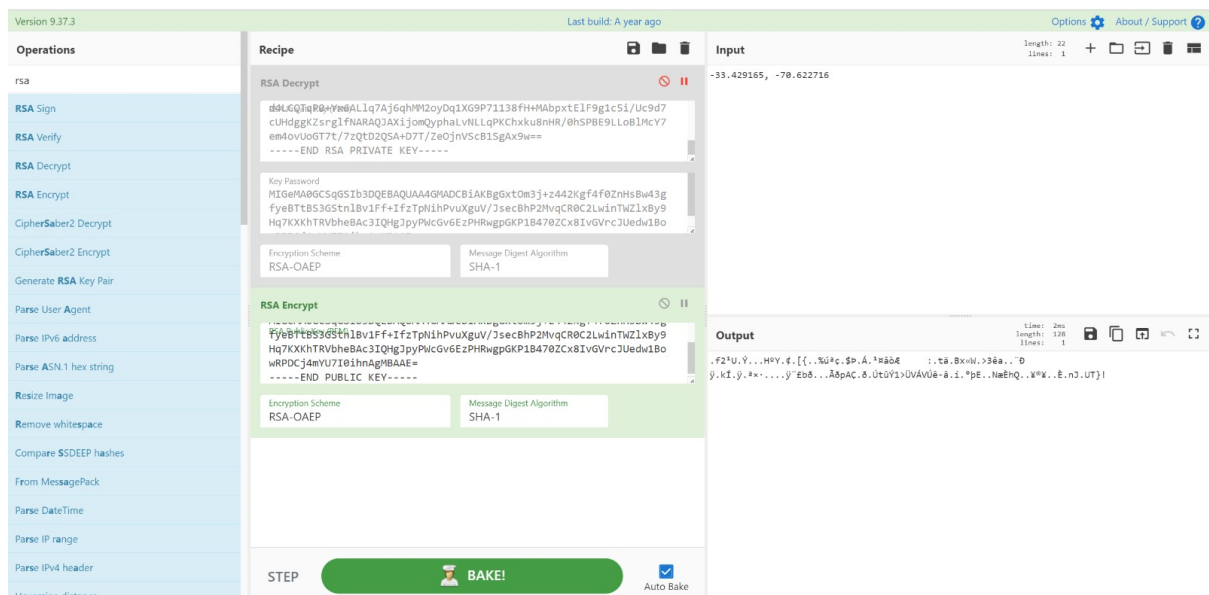
length: 22 lines: 1

-33.489742, -70.513682

STEP **BAKE!** Auto Bake

#### Paso 4. Sustitución y entrega de la tarea

Una vez se obtuvo el acceso a las coordenadas, se procedió luego a reemplazar esta información. Las coordenadas escogidas para ser reemplazadas fueron unas que conducen a una tienda de “Pokémon” cerca de la estación de metro “Manuel Montt” en la ciudad de Santiago de Chile. Utilizando la herramienta de RSA Encrypt de “Cyberchef”, y con la llave obtenida del .pdf, se encriptan las nuevas coordenadas y posteriormente se descargaron los archivos. Una vez realizada esta acción se da por finalizada la actividad.



Version 9.37.3 Last build: A year ago Options About / Support

**Operations**

- rsa
- RSA Sign
- RSA Verify
- RSA Decrypt
- RSA Encrypt
- CipherSaber2 Decrypt
- CipherSaber2 Encrypt
- Generate RSA Key Pair
- Parse User Agent
- Parse IPv6 address
- Parse ASN.1 hex string
- Resize Image
- Remove whitespace
- Compare SSDEEP hashes
- From MessagePack
- Parse DateTime
- Parse IP range
- Parse IPv4 header
- Haversine distance

**Recipe**

RSA Encrypt

Input

Length: 22

Lines: 1

-33.429165, -70.622716

File icon

Name: CTF01-coordenadas-iniciales.dat

Size: 128 bytes

Type: unknown

Loaded: 100%

Output

start: 0 time: 2ms

end: 22 length: 138

length: 138 lines: 1

f2\*U...HVV...f[...%c...\$p...Á...Hââ... :.tâ.BxwU...>3â...Dÿ.kI.j...%...j'EbB...ÂpAC...8.UtôY1>UVAVÜë-â.i.\*pE...NaEHQ...xW...È.nJ.UT}I

STEP **BAKE!** Auto Bake

## Anexo.

