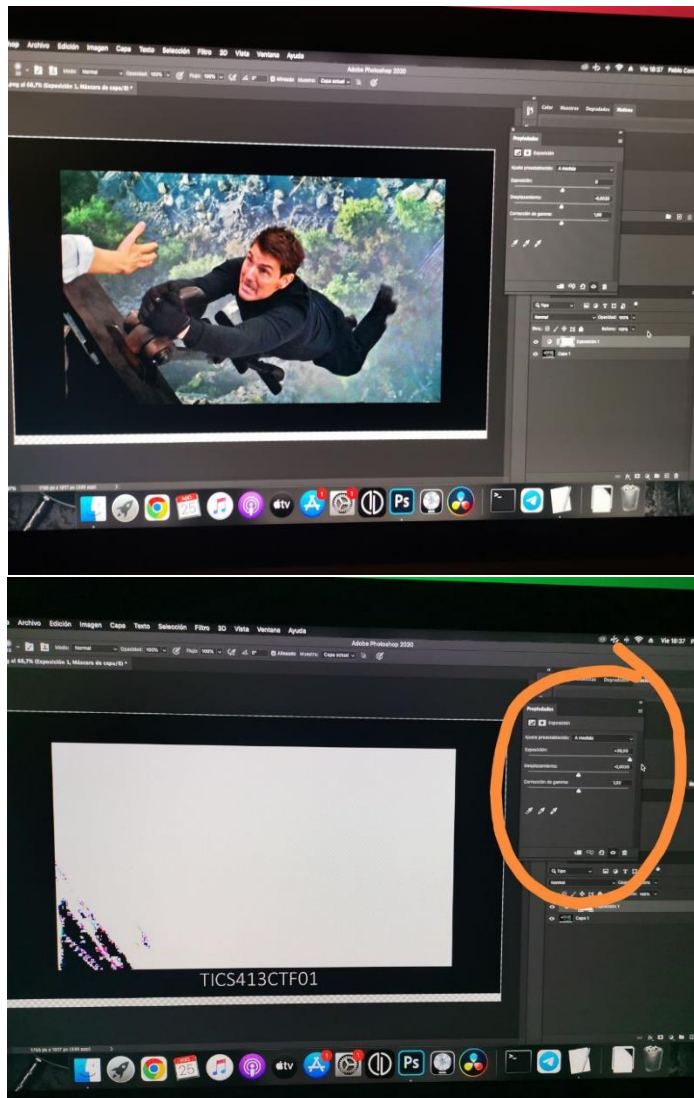
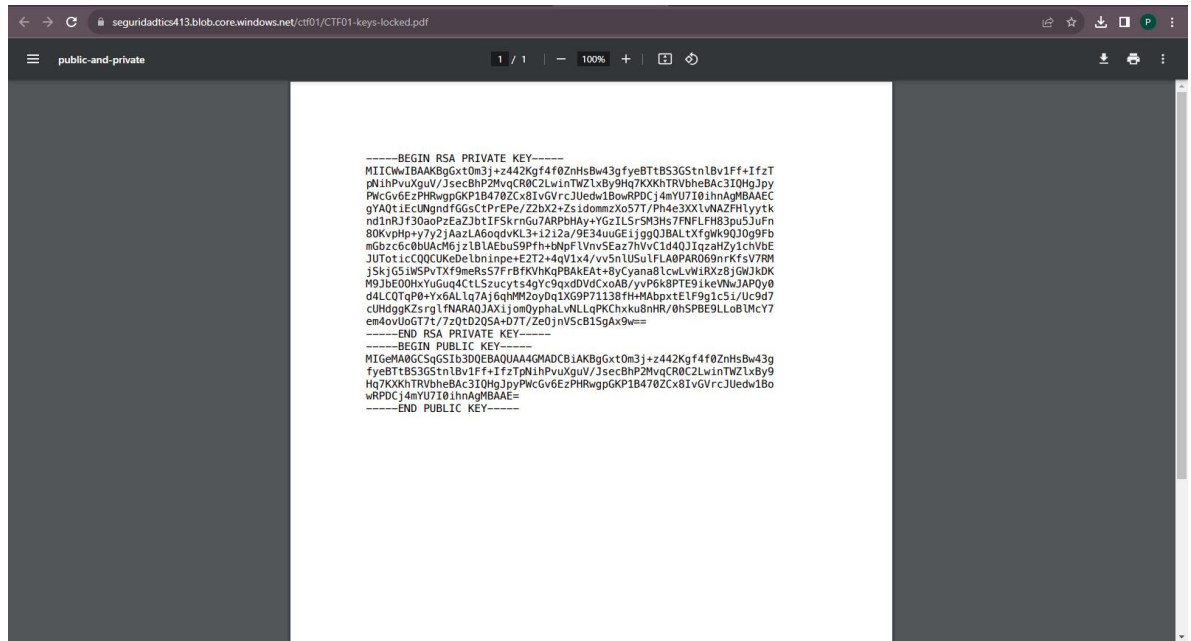


# Paso a paso CTF01 – Pablo Contreras Jorquera

1. Análisis de esteganografía: al observar me di cuenta de que podría tener un mensaje incrustado en la imagen, antes de analizar el archivo revisé la imagen en Photoshop y ajuste ciertos parámetros, especialmente la exposición. Al aumentar este parámetro apareció el texto: “TICS413CTF01”.



- Luego, ingresé ese texto al archivo con contraseña que me llevó a un archivo .dat con las claves pública y privada de RSA.

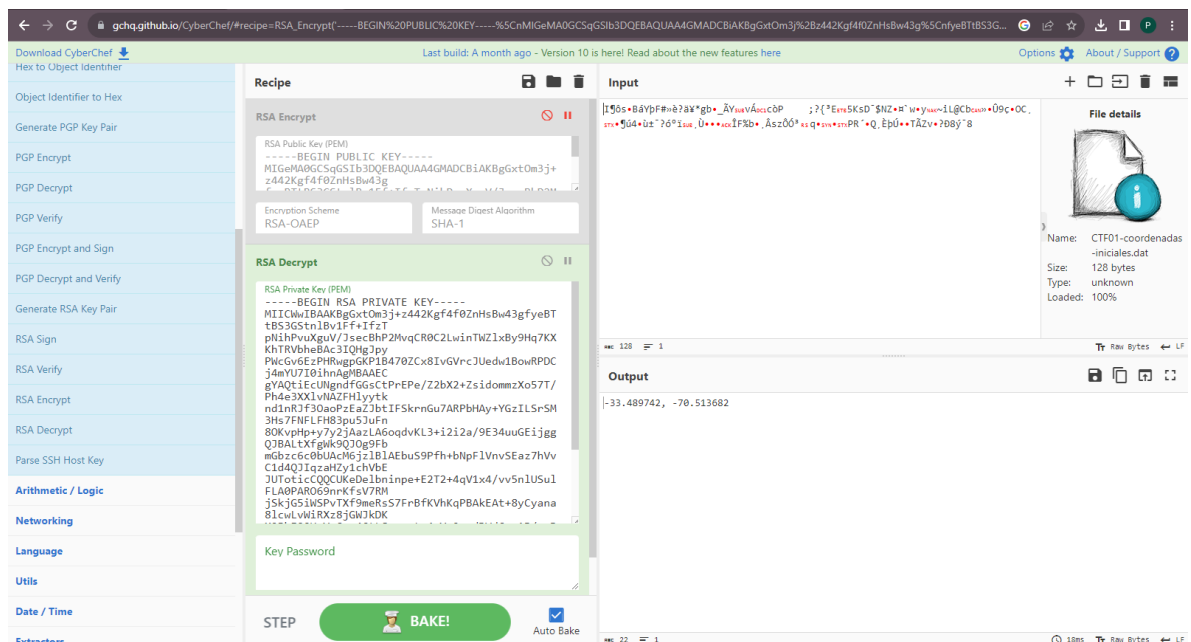


The screenshot shows a PDF document titled 'public-and-private' with the following content:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKAgGxtOm3j+z442KgF4f0ZnHsBw43gfyeBTtBS3GStnLbV1Ff+IfzT
pN1hPvuXguV/JsecBhP2MvqCR0C2Lw1nTWZLxBy9Hq7KXKhTRVbheBAC3IQHgJpy
PwC6v6EzPHRwggGKPB470ZC81vGVrcJuedw1B0wRPOCj4mYU7I01hnaqMBAAEC
gYAQI1eClUgndfGGSctPrEPe/Z2bX2+Zs1dommzXo57T/Ph4e3XX1vNAZFHL1yYtk
nd1nR3f30aoPzEaZJbtIFSkRnGu7ARPhAY+YgZILS5rSM3Hs7FNLFH83pu5JuFn
8OKvpHp+y7y2jAazLA6oqdVKL3+i2i2a/9E34uuGE1jggQJ8ALTxfGwK9QJ0g9Fb
mGbzc6c0BUAcM6jz1B1AEbu59Pfh+bNpF1VnvSEaz7hVvC1d4QJ1qzaH2y1chVbE
JUTot1cCQ0CkEde1bninpe+E2T2+4qV1x4/vv5n1U5u1FLA0PAR069nKfsV7RM
j5kG51WSPvTXf9meRS7FrBfKVhKqPBkAEAT+8yCyana81cwlwJRKz8JGwJ0K
M9JbE00HxYuG04CtLSzucyts4qYc9qxdVDCxoAB/yvP6k8PTEf091c51/Uc9d7
d4LC0TqP8+Yx6AL1q7aj6qHMM2oyDq1XG9P71138fHhMAbpxTEf091c51/Uc9d7
cUHdgKzrg1FNARQJAXIjom0yphALvNLLqPKChxku8nHR/0hSPBE9Ll0B1McY7
em4ovd0GT7/7z0tB2Q5A+D7T/Zed0jnV5cB15gA9w==
-----END RSA PRIVATE KEY-----

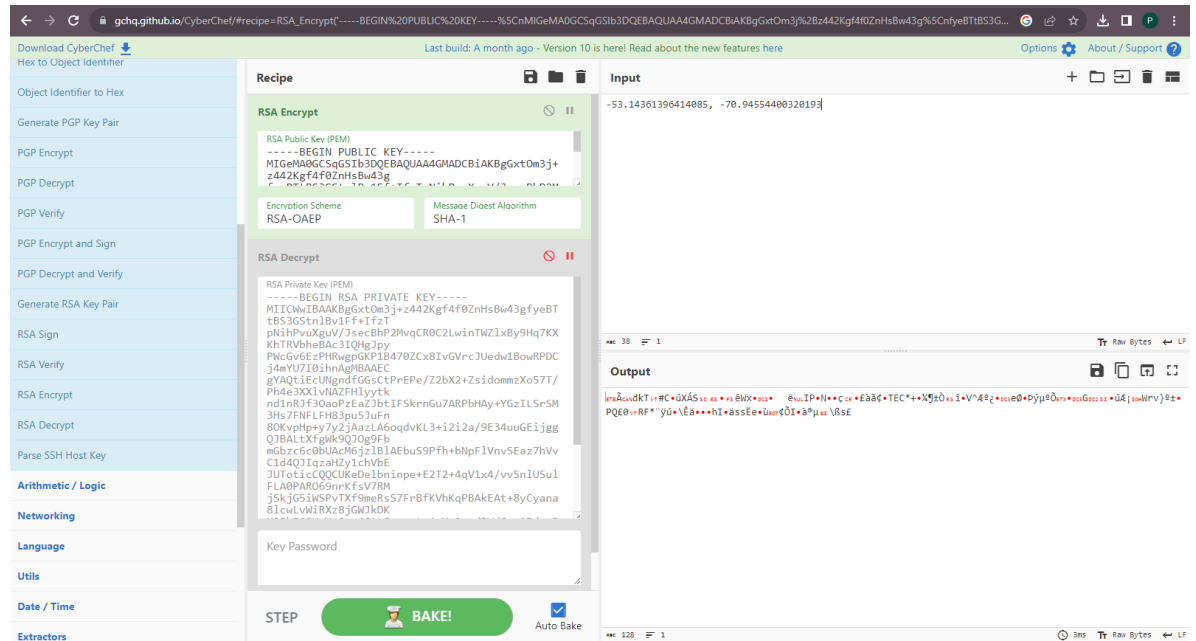
-----BEGIN PUBLIC KEY-----
MIGeMA0GCsqG5Ib3DQEBAAQAA4GMADCBIAKAgGxtOm3j+z442KgF4f0ZnHsBw43g
fyeBTtBS3GStnLbV1Ff+IfzTpN1hPvuXguV/JsecBhP2MvqCR0C2Lw1nTWZLxBy9
Hq7KXKhTRVbheBAC3IQHgJpyPwC6v6EzPHRwggGKPB470ZC81vGVrcJuedw1B0w
RPOCj4mYU7I01hnaqMBAAE=
-----END PUBLIC KEY-----
```

- En el sitio Cyberchef pruebo ambas claves y el archivo .dat, para corroborar su funcionamiento, entregando las coordenadas del Edificio E de la UAI.



- Ahora elijo una coordenada aleatoria para cambiar el lugar de entrega. Las coordenadas son: -53.14361396414085, -70.94554400320193; que corresponde a la

ciudad de Punta Arenas. Encripto la información usando la llave pública del archivo con contraseña.



5. Exporto el mensaje encriptado, generando un archivo llamado nuevascoordenadas.dat.
6. Finalmente corroboro si se puede desencriptar con la llave privada.

