Entrega final - Seguridad informática - IFTS 16
Profesor: Diego Rende
Alumno: Matías Maglio

Instrucciones para probar el chat:

El chat funciona mediante la ejecución de archivos de Python 3. Ya sea en el entorno global o creando un entorno virtual de python se necesitan instalar las siguientes librerías, si no están ya instaladas

- Para el encriptado:
  pip3 install rsa

- Para la GUI:
  pip3 install tk

También se usan las librerías socket y threading pero entiendo que esas ya vienen con python.

Para probar el chat se debe ejecutar desde python el archivo server.py para iniciar el servidor (corre en el puerto 9090) y después en otras dos instancias separadas, el archivo client.py

Consideraciones (leer porfa):

- El chat y el encriptado funcionan, pero tengo un bug que no llegué a arreglar donde a veces, al hacer clic en “enviar”, el mensaje no se envía. Después de volver a apretar el botón un par de veces el mensaje se envía pero a partir de ahí el chat deja de funcionar como debería, es como si el mensaje quedase en una cola o algo así. Voy a seguir investigando como arreglarlo pero para la entrega del final así es como llegué a dejarlo. Igualmente, entiendo, el cifrado funciona bien.

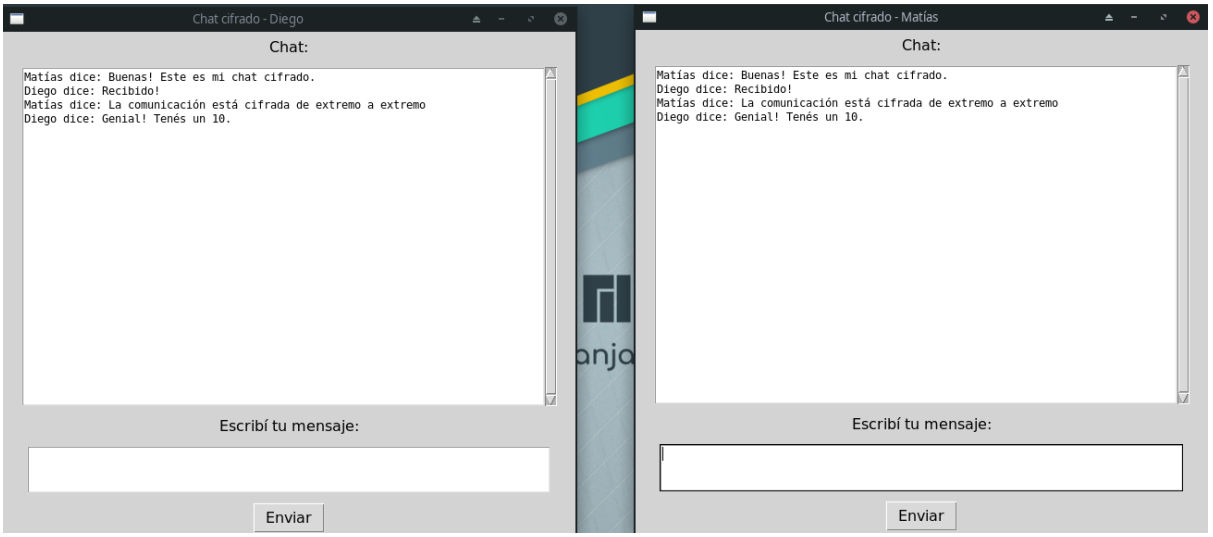
- Para que el chat funcione, hay que inicializar los 2 clientes antes de enviar algún mensaje. Si el cliente 1 envía algún mensaje antes de que el cliente 2 se conecte, el programa se rompe.

- El chat admite solo 2 clientes.

- Deje algunas líneas de comentarios en el código explicando cómo funciona, sobre todo, el encriptado. Además agregué unas impresiones en la consola para mostrar algunas cosas como que la clave pública llega al servidor y que el cliente logra encriptar el mensaje antes de enviarlo.

Entrega final - Seguridad informática - IFTS 16
Profesor: Diego Rende
Alumno: Matías Maglio

Imagenes de muestra:




```
[zafiro@zafiropc SeguridadInformatica]$ python3 server.py
Servidor iniciado...
Conectado a('127.0.0.1', 52186)

El nick del usuario es: Diego

Su clave pública es:
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMrCiqy0EyPvUjf3xvY3LlOZpIFCUSzvXhrBNQ/2E34Vy+ilmOCBfNiS
cVFCkug1IxHyVufWUn6GtgwuM6GJf3ptxfYQGfXE7jmtBdB0jSXTma2iwmgOLKcb
FA779tEJ22YCXz/7daEIfJPFU/5nheoLtxNUZGt46Aydm1zeOnLTAgMBAAE=
-----END RSA PUBLIC KEY-----

Conectado a('127.0.0.1', 52190)

El nick del usuario es: Matías

Su clave pública es:
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAISOIgzvh4aoKcRV6FQMnK3MDsQ4BLIJZ9+mknM67d0rTycl2iwnnDM9
YSwTSe5tIJH1o1pfil1BwsTwLVBZAH0nVxjXFxtIxYT4uDkVy+hQbXe+Q6brf5a5
z8WiPcpfYt3QJEZcNTW+Ah0eiJP1KCrW0EPqDWPvRttoAGDkUY1hAgMBAAE=
-----END RSA PUBLIC KEY-----
```

```
[zafiro@zafiropc SeguridadInformatica]$ python3 client.py

Este es el mensaje encriptado:
b's\xc6\xa0\xc5r\xeb\xf3]PQV ,w\x98\xc9b\xbb\xbe\xa5\x00\xfe"\xdek\xfc\xbd\x823\xe2Sxh\xe9S\xc1\xc3\xd4$w4K"\x95\x85-\x1aJ\xdfh\xd0]\x1
8\x82[\x92\xf3v\xab<tf@\xe1\xb8zWW\xa7\xe4\xf3\xe0\x13+\x94\x99uB\xe5\xcb\x8d\xc4{\xf4\xc3\xa2\xa5j\xb9\xe29\xd3\x08\xe3-4>\x8e\xc7\xc7
\xf9\x0e\xec\x0f\x98\x98\xb6\xc7\x8c\xfdVY.\xd6\xd1\xe6I#\xdd\xe1\x1fpW\xb1s\xe1\xf6\x8b'

Este es el mensaje encriptado:
b'!tq6N=\xee\x83I\xa2\xf3r\x1b@Ju\x89\xf2qW\xc9\x85m\xc6T\xd9b\x8d-tI,\x86\x84ro\xaf\x94\xde\x15fi\xe3\xdc\x94\x9f*3\x0b1>\x9c\x07\xc9\
xbb\x12Y\xd0%=\x0e4\x1c\xdd\xc4\x8d\xd19\xf6\xef\x16\x1b\xdd\x1c\xc6EI\xda\xbeD(\x01\xb2\xb6\x06<\xa6\x9f[\x17ix\xafo\x07\x93g\x16\x96
\xdc\x06[\x06~c\xebe\x9f1\x13\x00\x90\x8e5\x15\x0e:\x94\x160b\x9a\xb2M\x9c-j'
```