CMPT 471 Networking II - Group Project
End-to-end encryption chat application

Huaicheng Deng 301313726 hda25@sfu.ca
Handi Yang 301341169 hya71@sfu.ca
Instructor: Khaled Diab

Objective:

1. Implementing a chat application establish communications between client
2. The messages sent between client ends are encrypted using RSA
3. The application should be supported by the user interface

Work Distribution:

- Huaicheng Deng:
  - Implemented original **server.py** and **client.py** programs
  - Advanced **client.py** to fit the modified **server.py** (by Handi Yang)
  - Encapsulate the original send process into functions **send_display()**, **receive_display()**
  - Designed and Implemented Tkinter user interface features in **client.py**
- Handi Yang:
  - Advanced **server.py** based on the original program (by Huaicheng Deng)
  - Designed and Implemented encryption features in **crypt.py** file
  - Implemented the encryption features within **server.py** and **client.py**
  - Implemented the auto-receiving feature in the **client.py**

Known Issues Or Bugs:

- Blocked by input issue has been found, which is handled by the user interface button

Lesson Learnt

- **Huaicheng Deng:**

The final project requires group works to complete the desired objectives. Not only personal abilities are evaluated, but also the skills of collaboration are examined. We distribute the work based on members' knowledge to assign the most suitable tasks for group members, which improve the skills of communication and problem analyzing. During the process of implementing and debugging, we help each other to come up with creative solutions toward the incoming problems and achieve the goal of the project. With the specific RSA encryption technique, we have learnt while producing the project, more importantly, the trusts have been developed among group members through the entire process of implementation.

- **Handi Yang:**

The motivation of the chat application is based on the importance of private information transmission, which the secure message sending process should be guaranteed to protect the clients. The RSA technique we have implemented provides safe message transmission between clients based on the public key and private key. During the implementation process, we found a lot of concurrency problems that could be solved more efficiently with multithreading. But unfortunately, due to the complexity of implementation and limited times available, we gave up on muti-threading and chosen another easier method to implement. Besides the encryption technique, our skills in team working are improved during the process of application development. It is important to declare the problems so that we can figure out the best solution to get over the difficulties.