RSA-algorithm

RSA implementation using python

How to Run?

1. make sure you have the following libraries:
   - math
   - socket
   - Crypto
   - os
2. open two terminals
3. run server.py using the following command: python server.py ,in the first terminal
4. run client.py using the following command: python client.py ,in the second terminal
5. start chatting on the client side "both client and server can send and receive but the client starts the sending"

To Run the attack code (attack.ipynb)

1. make sure you have the previous libraries in addtion to the following ones:
   - time
   - matplotlib.pyplot
2. run each cell in order
3. the final output is a graph represents the relationship between the number of bits of the key and time taken to attack the algorithm

Files

1. main.py : contains all the functions implementaions and all the imports
2. server.py: contains the server code that establish the connection
3. client.py: contains the client code that connects with the server
4. attack.ipynb: contains the Brute-Force Attack and Fermat factoring algorithm Attack code.