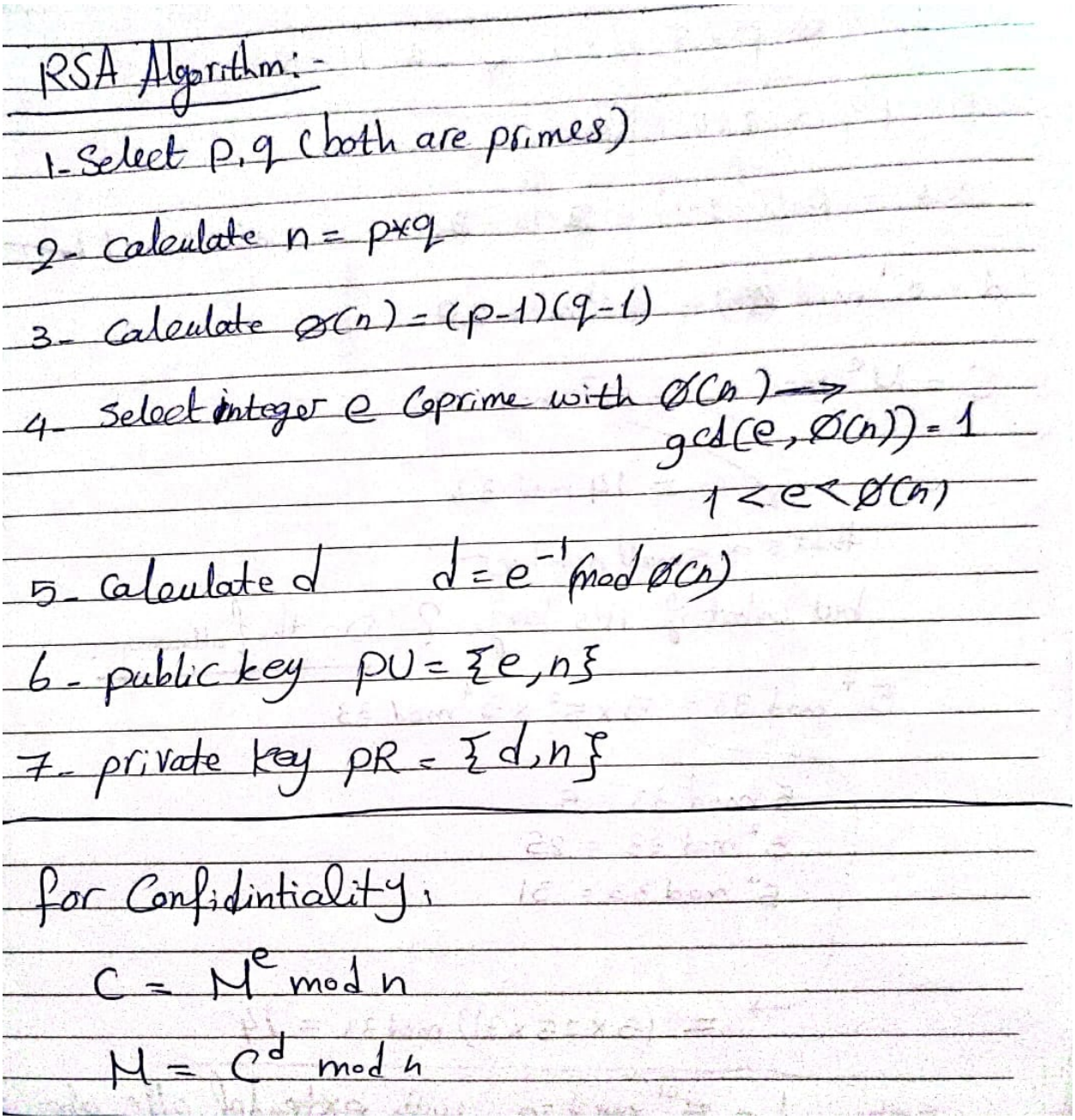
Project Report

Name: Abeer Hussein Mohamed section: 1 BN: 34

Implementation of RSA:

I implemented it like the textbook



Implemented the communication using python socket.

Why the CCT happens: because the decryption of C-dash (the cipher with another random number) = Y ,is easy due to the fact that e and d are inverses so Y = M*r mod n

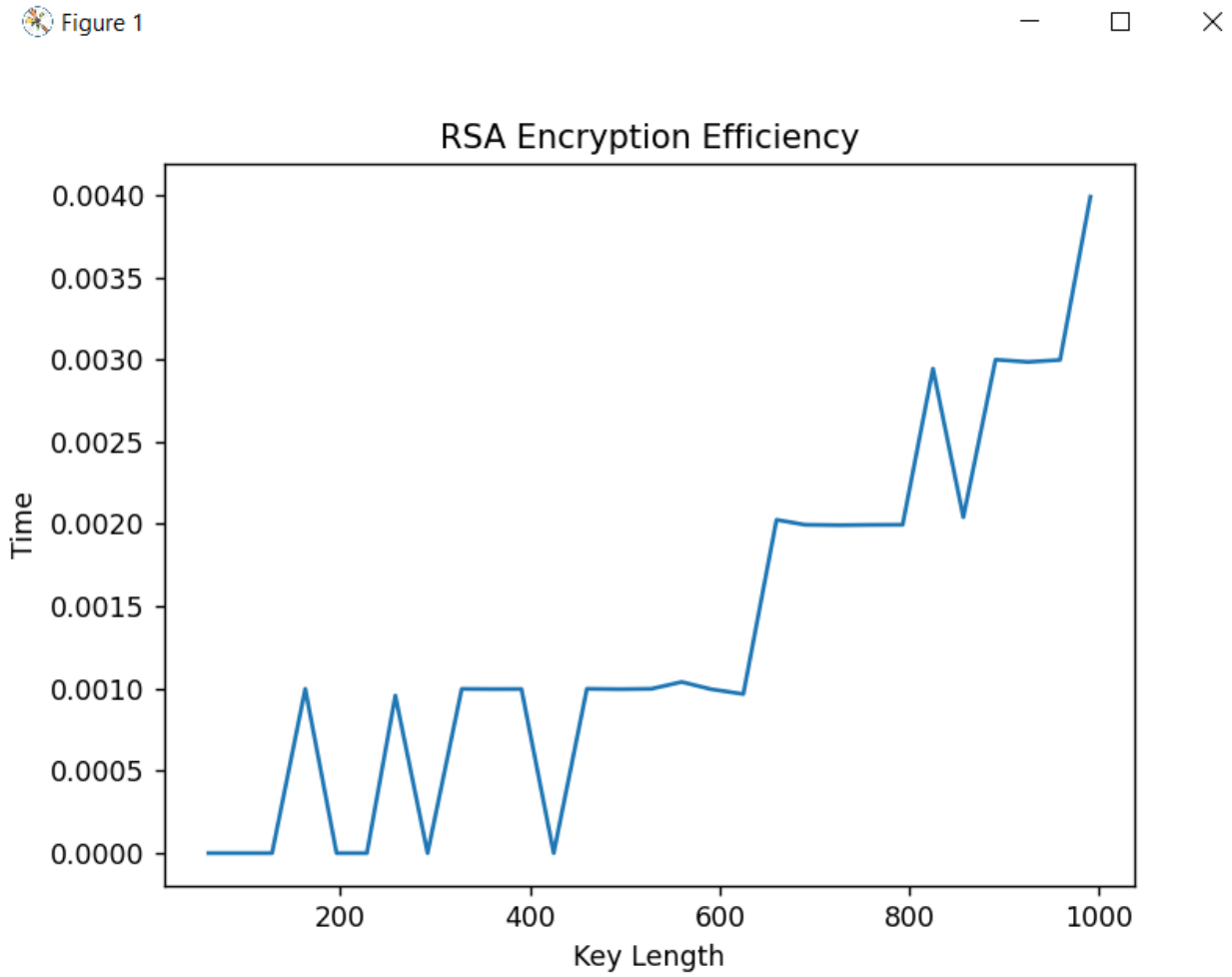


Figure 1
RSA Encryption Efficiency
Time
0.0040
0.0035
0.0030
0.0025
0.0020
0.0015
0.0010
0.0005
0.0000
200
400
600
800
1000
Key Length

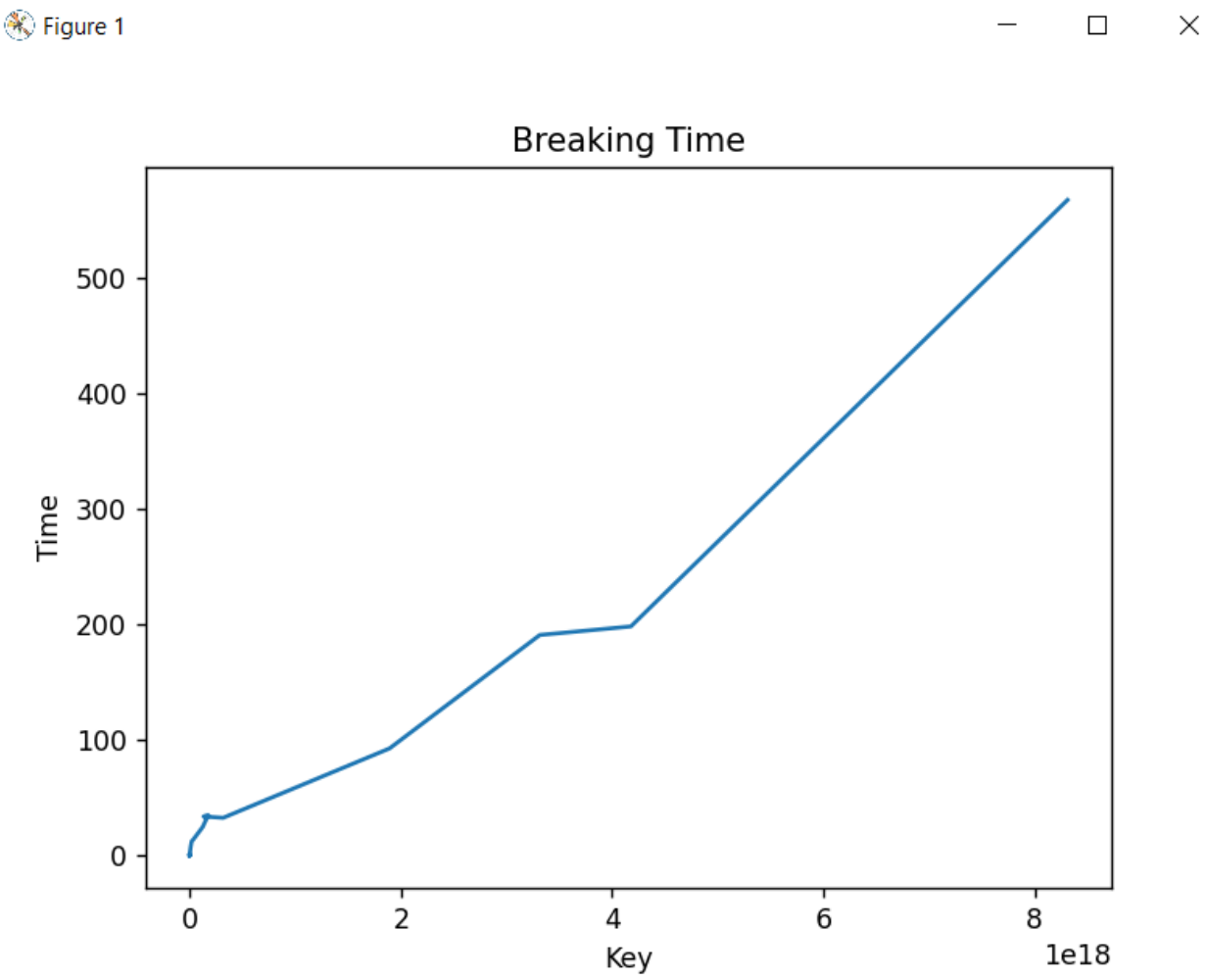


Figure 1
Breaking Time
Time
500
400
300
200
100
0
0
2
4
6
8
Key
1e18