RSA Assignment

Samaa Hazem Mohamed Abdel-latif
Sec: 1
BN: 32
Code: 9202660

Our analysis is divided into 2 parts, efficiency of RSA algorithm in terms of encryption and decryption speed, and the difficulty of attacking in terms of time-n size.

Encryption and Decryption Analysis

In the following two screenshots resulted from **enc_dec_Analysis.py** ,we notice that even we reach to 3000 bits at the size of public key (n) that the encryption and decryption does not almost exceed 0.08-0.09 sec , which is very good ,see the end of the report to compare it with attack time.

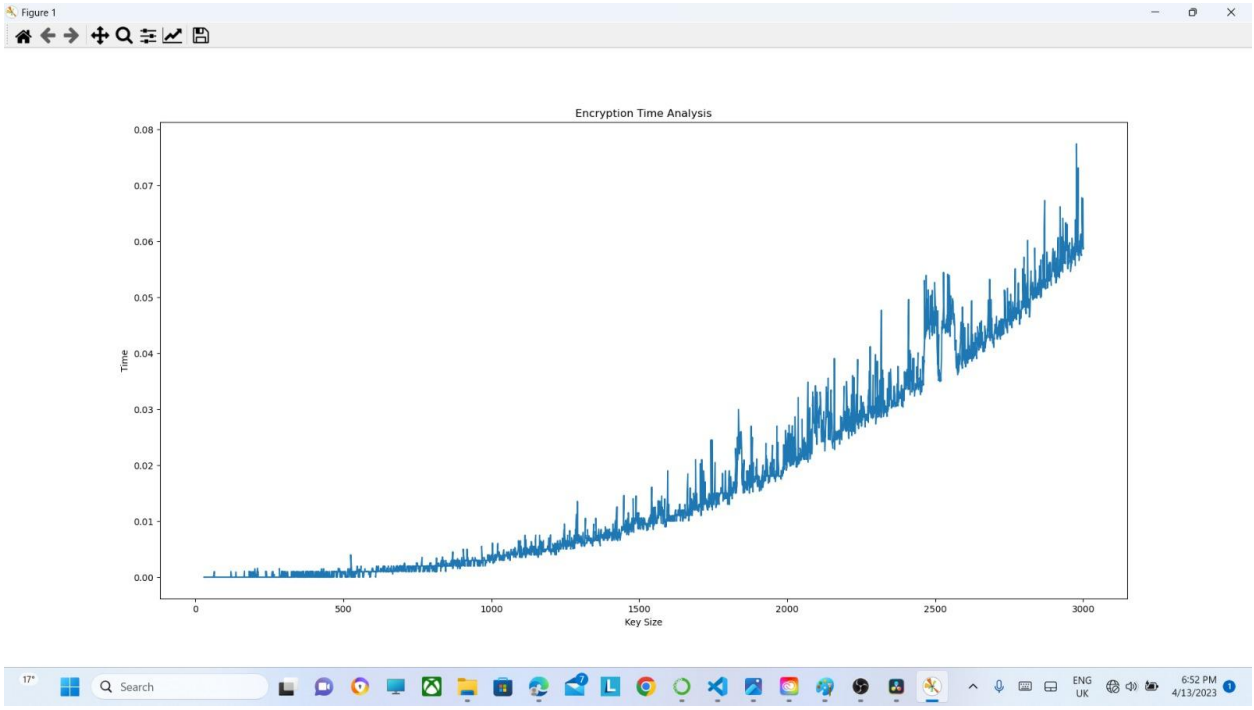


Figure 1
Encryption Time Analysis
Time
Key Size
0.00
0.01
0.02
0.03
0.04
0.05
0.06
0.07
0.08
0
500
1000
1500
2000
2500
3000
Search
ENG
UK
6:52 PM
4/13/2023

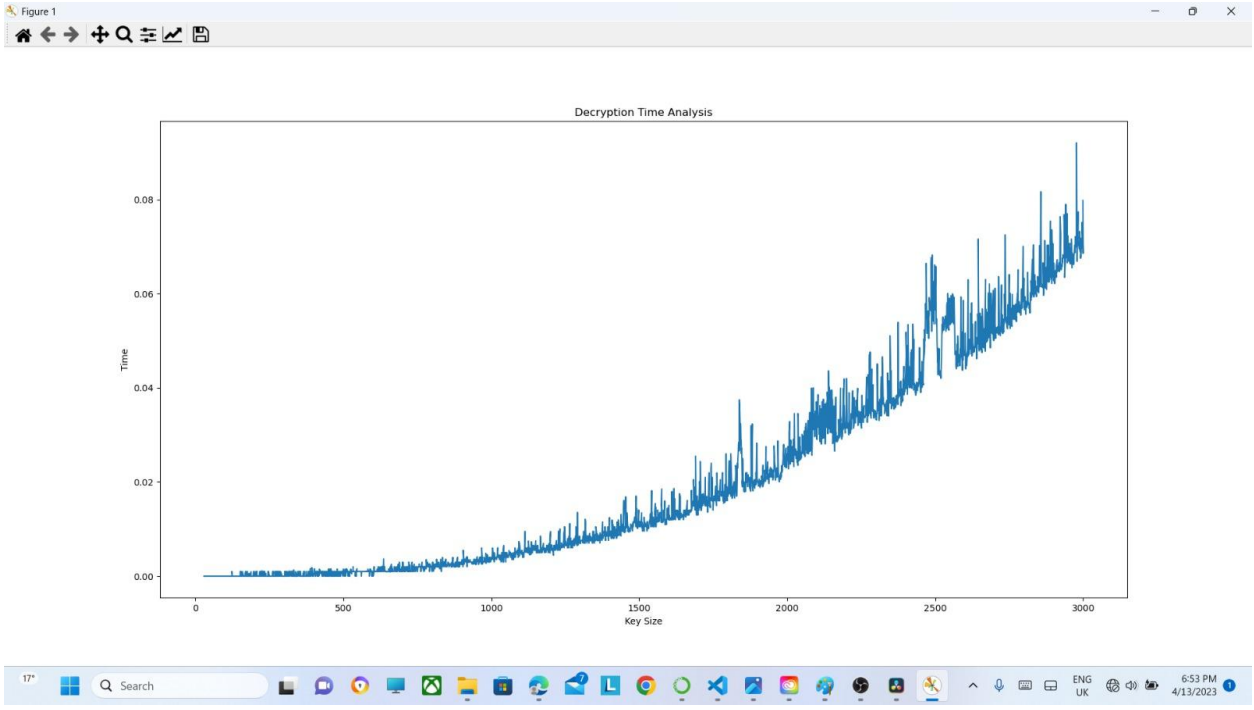
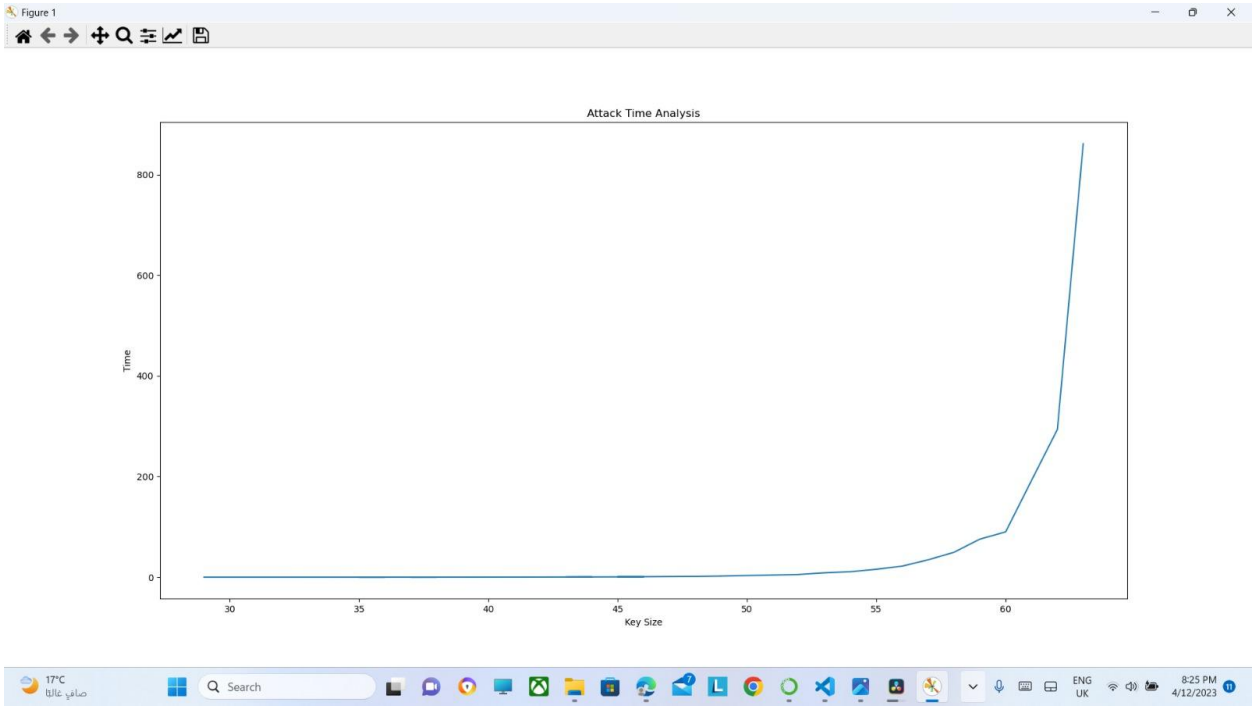


Figure 1
Decryption Time Analysis
Time
Key Size
0.00
0.02
0.04
0.06
0.08
0
500
1000
1500
2000
2500
3000
Search
ENG
UK
6:53 PM
4/13/2023

Attack Analysis

To analyze the power of the RSA encryption/decryption algorithm focused on factorizing problem of public key (n) to its two prime factors when getting large, we notice that for key size = 63 , the attack took 800 sec !!
What if it reaches to size 3000!!!



Comparing time needed to encryption/decryption with the attacking time , increasing size of (n) does not affect the time of encryption/decryption obviously, unlike the time of attacking which starts to increase even exponentially in range 55-60 already.
So having the power of factorizing will not really affect the time for communication.