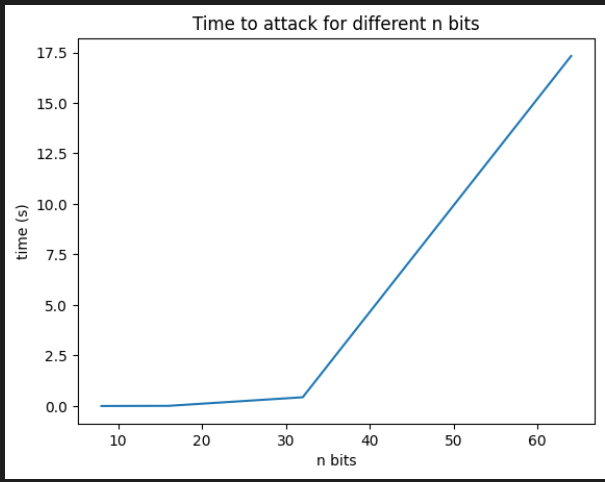
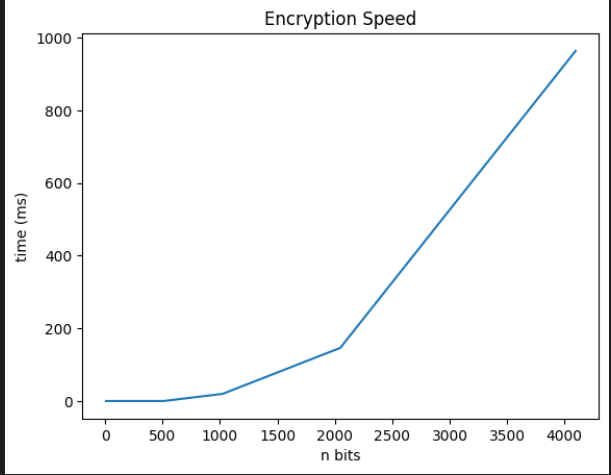
RSA Assignment Report

Results:

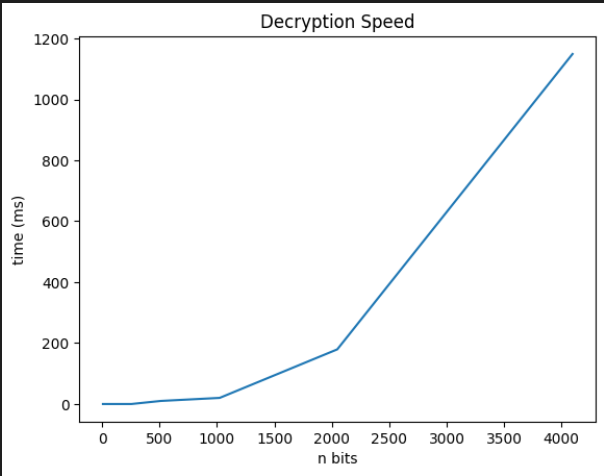
* Time of algorithm breaking
  + We can see that:
    - For small n 🡪 the change in time is small.
    - For large n 🡪 the change becomes large and linear.



* Speed of encryption
  + We can notice that:
    - For small n 🡪 the change in time is relatively small.
    - For large n 🡪 the change in time increases gradually untill it becomes linear.
    - But here the change in time become large at larger ranges of n than in case of the algorithm breaking which make sense.



* Speed of decryption
  + From the figure below we can see that:
    - The speed of decryption is very similar to the speed of encryption.



Conclusion:

It is better to keep n as large as possible so that we avoid attacks and preserve the algorithm from being broken.