RSA Assignment Report

Made by:

Doaa Magdy Ibrahim Mohamed

Supervised by:

Eng. Khaled Moataz

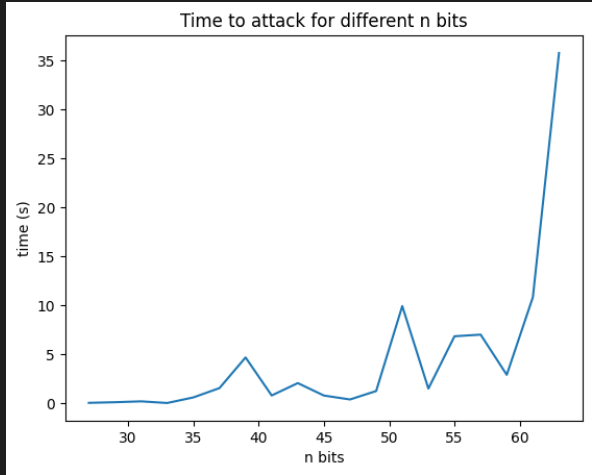
Dr. Samir Shaheen

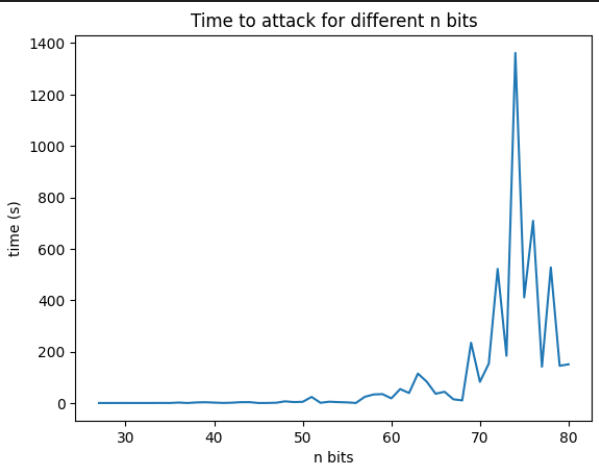
Course: CMP3050

B.N.: 24

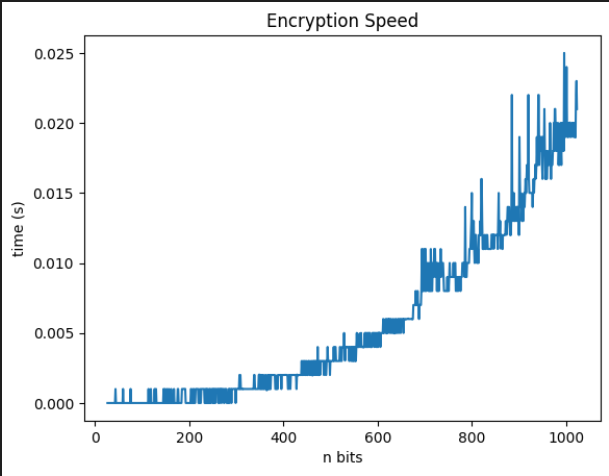
Results:

* 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 the graph tends to take the exponential shape.
    - And from the second graph, we can see that at some large n\_bits the time can decrease. This makes sense cause the factors may be found earlier and then the time becomes small.

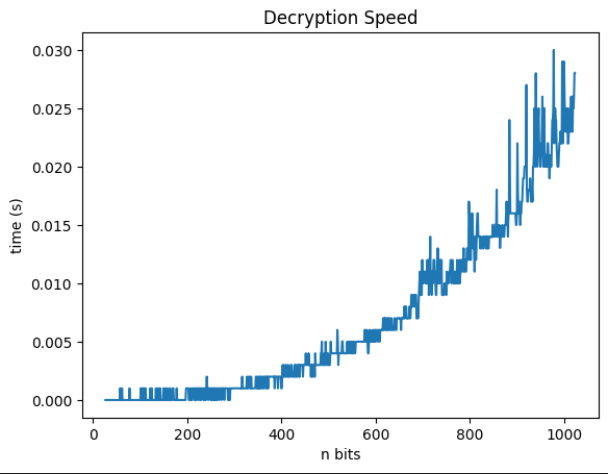




* Speed of encryption
  + We can notice that:
    - For small n 🡪 the change in time is relatively small.
    - For large n 🡪 the change in time increases gradually.
    - The graph takes the exponential shape



* Speed of decryption
  + From the figure below we can see that:
    - The speed of decryption is very similar to the speed of encryption.
    - The speed of decryption and encryption is larger than the speed of breaking the algorithm which is as expected.



Conclusion:

It is better to keep n as large as possible so that we avoid attacks and preserve the algorithm from being broken as the analysis shows that as n gets larger, the time to break the algorithm gets larger too and the increasing is exponential.