Cairo University
Faculty of Engineering

Department of Computer Engineering

CMP3050 – Spring 2023

Cryptography

RSA project

Submitted to

Dr. Sameer Shaheen

Eng. Khaled Moataz

Submitted by

Name	Sec	BN
Nour Ziad	2	31

When doing time analysis over the encryption and decryption and the attacking algorithm we obtained the following results:

First of all, for encryption and decryption the performance of the algorithm was differing greatly with number of bits in the key

As shown in the figures

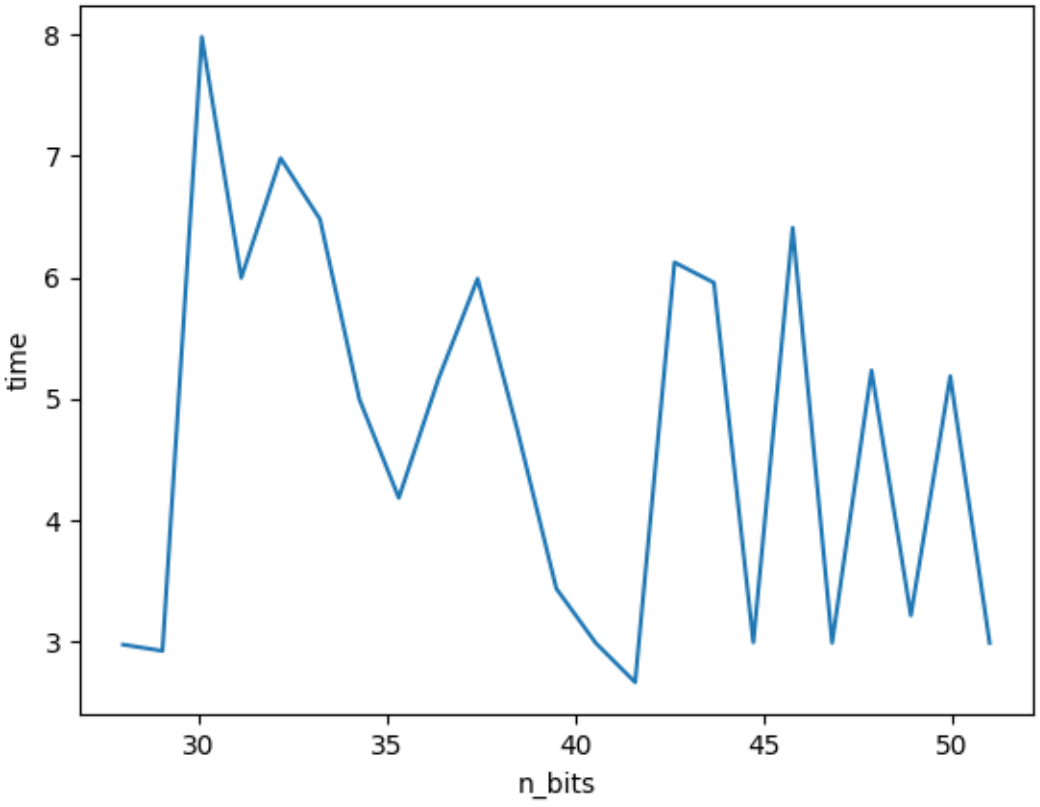
Although we can't say that number of bits in the encryption/decryption result in a huge change in time

We tried both algorithms on a kind of long message to obtain these results:

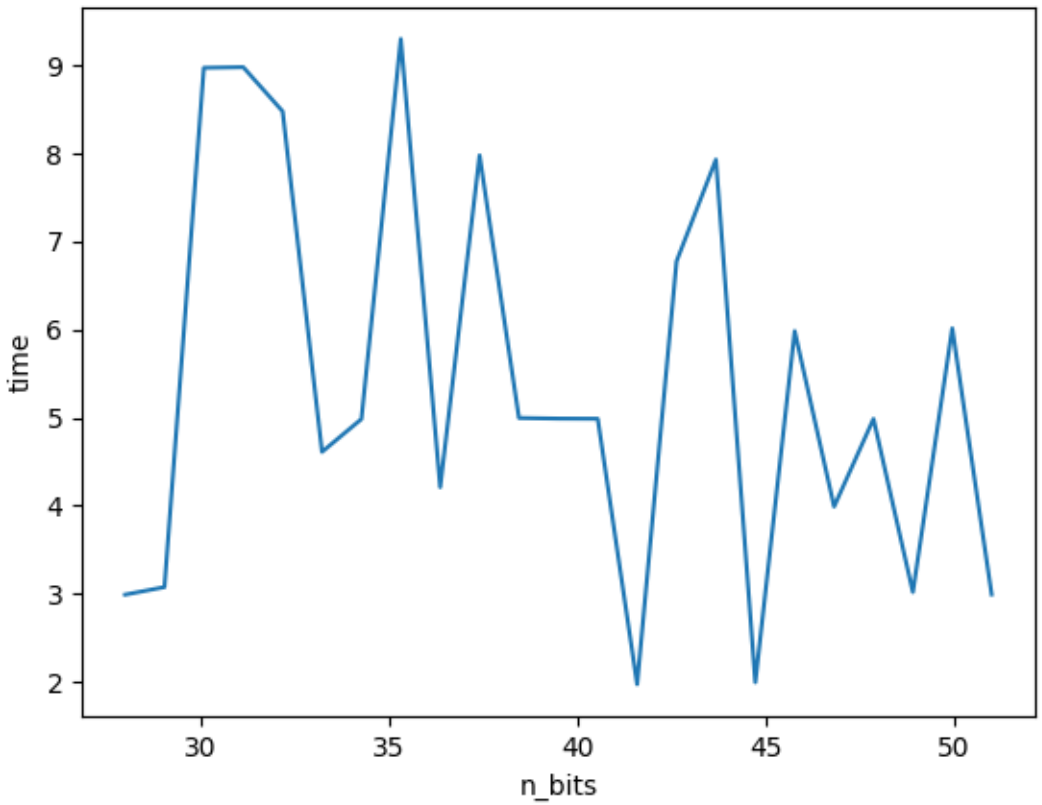
Msg : "`hello alice this is a message by bob, this is a very long message provided by me to tell you nothing important but to get an accurate analysis of my code, now i am trying to make it longer so i can get better estimate of time`"

Source code: https://github.com/nouralmulhem/RSA_Project

Encryption figure:



Decryption figure:



For the attacking algorithm it was obviously showed that the bigger number of bits used in the key result directly in increasing the complexity to attack the system the graph is increasing exponentially which makes it a very hard and time consuming mission when using large number of bits such as 64 bits

As shown in figure: