Cairo University
Faculty of Engineering

Department of Computer Engineering

CMP 3050 – Spring 2023

Cryptography and Network Security

Assignment #1

RSA

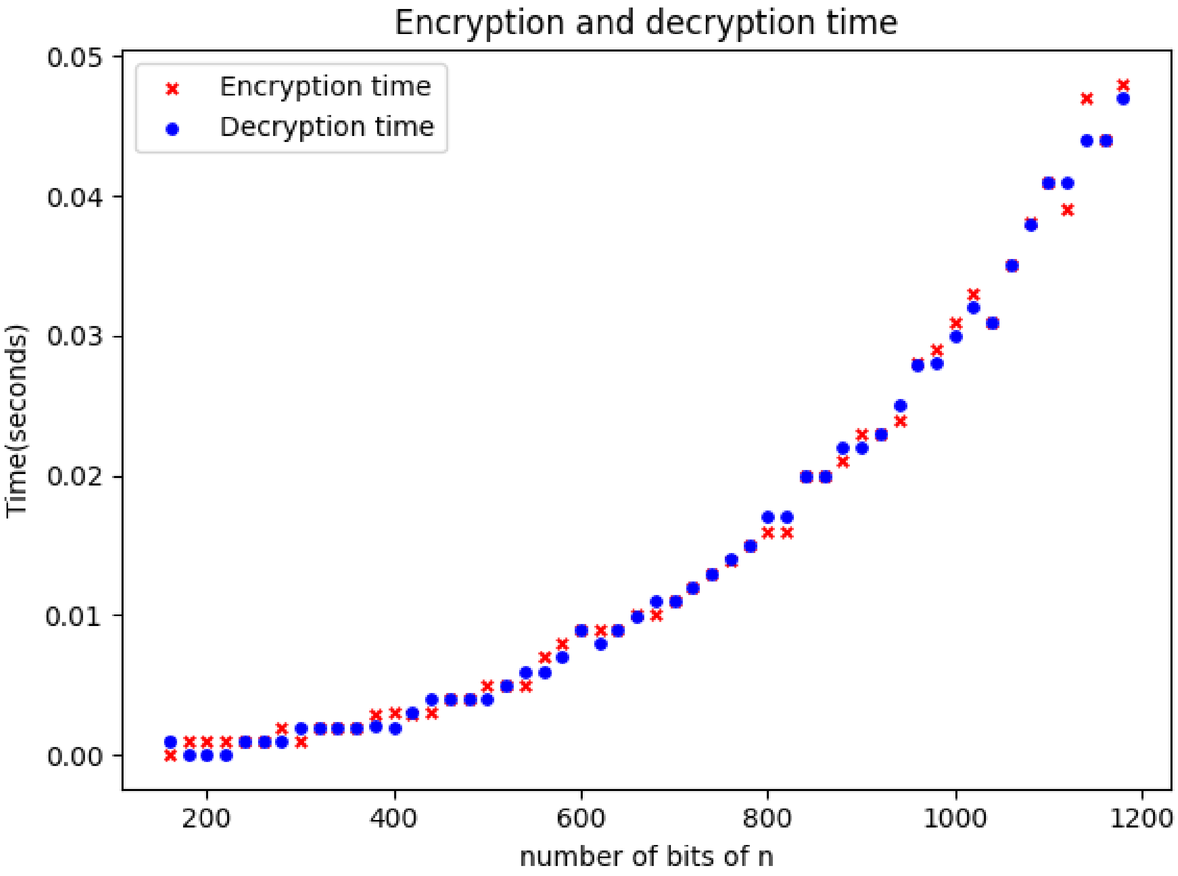
Submitted to

Eng. Khaled Moataz

Submitted by

Name	Sec	BN
Adham Ali Abdelaal	1	12

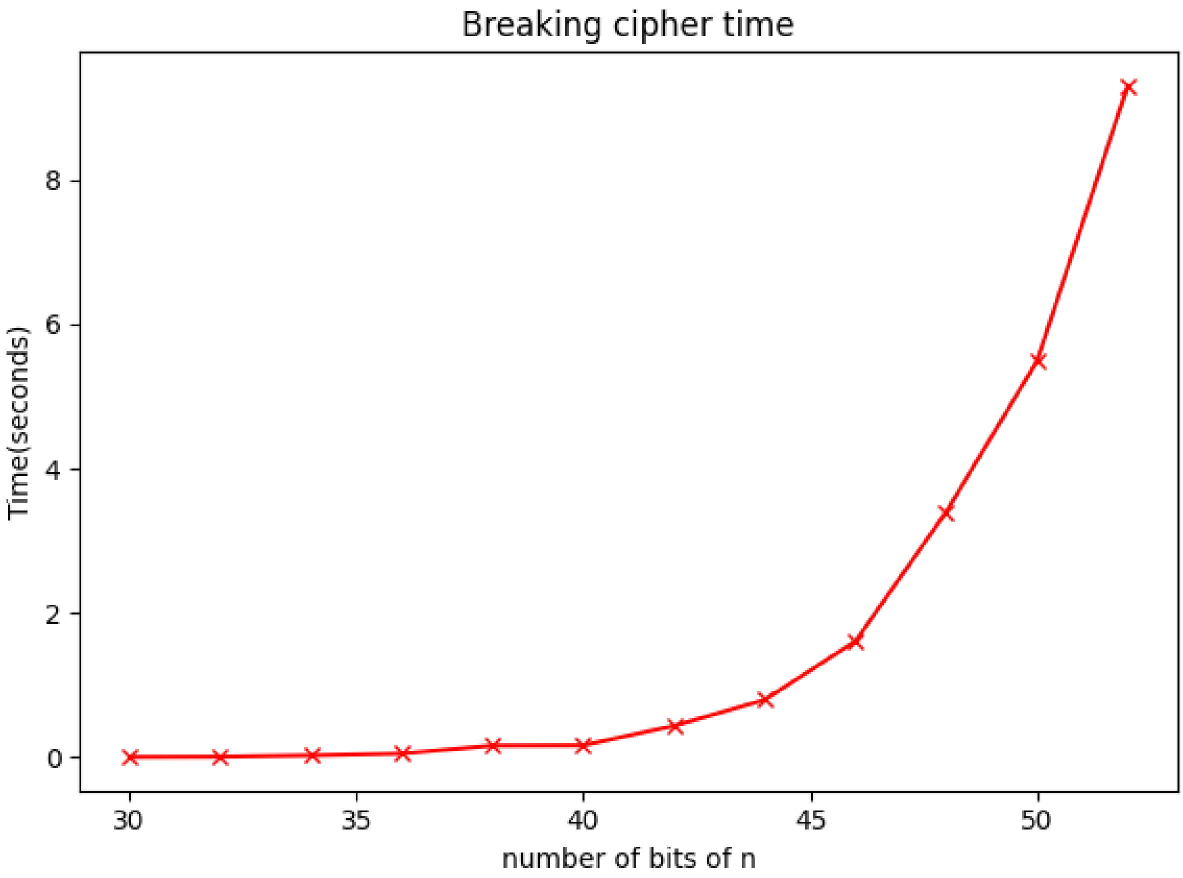
Part 1:



Comment:

As in the figure the encryption, decryption time and cost increase as the number of bits of n (which defines the key) increases but the time when number of bits = 1200 bit is almost 0.05 seconds or less which is very little time relative to the number of bits used that means that RSA is one of the most efficient encryption algorithms.

Part 2:



Comment:

The problem of breaking ciphertext in RSA encryption algorithm is in how to get d (private key) given e and n (public key) and to do that you need to factorize n to p and q to get fai = p * q then calculate d such that d is the inverse of e modulo fai(n) so the main problem is factorization of n into two large prime numbers. Now according to the figure as the number of bits of n increase the time to break the encryption increases exponentially which means that to break practically RSA with n has large number of bits it may take years or centuries that can be deduced by the figure as the time taken to break RSA with n has 50 bits is 8 seconds.