Cairo University
Faculty of Engineering

Department of Computer Engineering

RSA Assignment

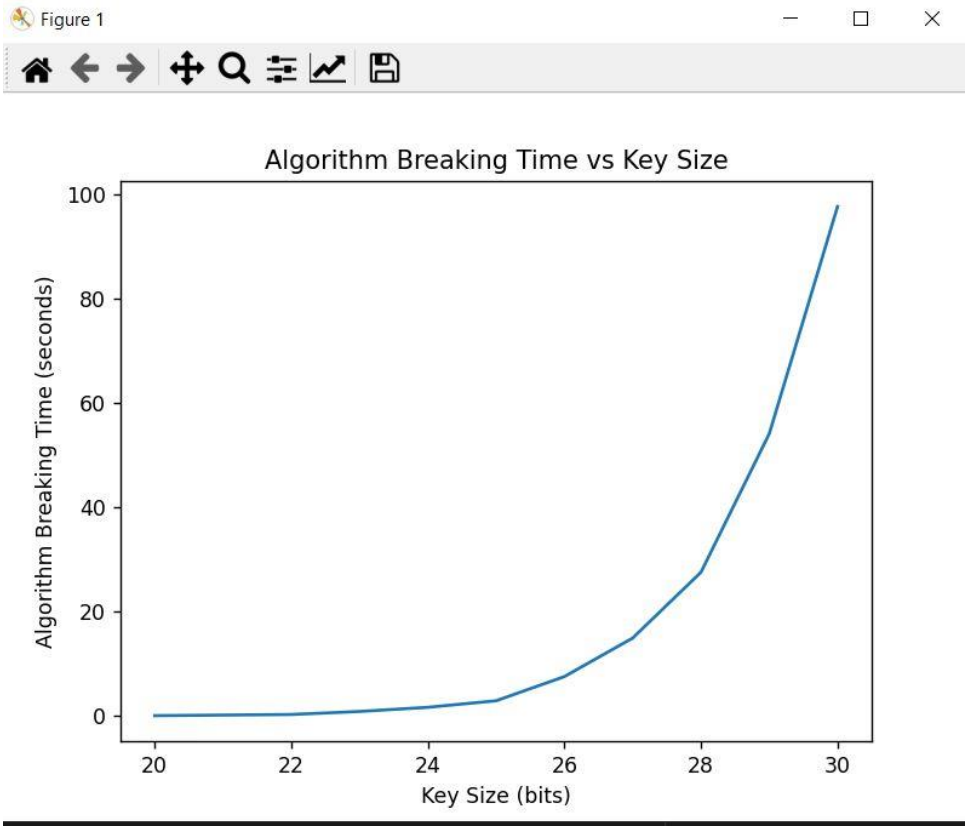
Submitted by

Abdelrahman Ashraf Mohamed

Sec: 1

BN: 35

Algorithm Breaking Time vs Key Size

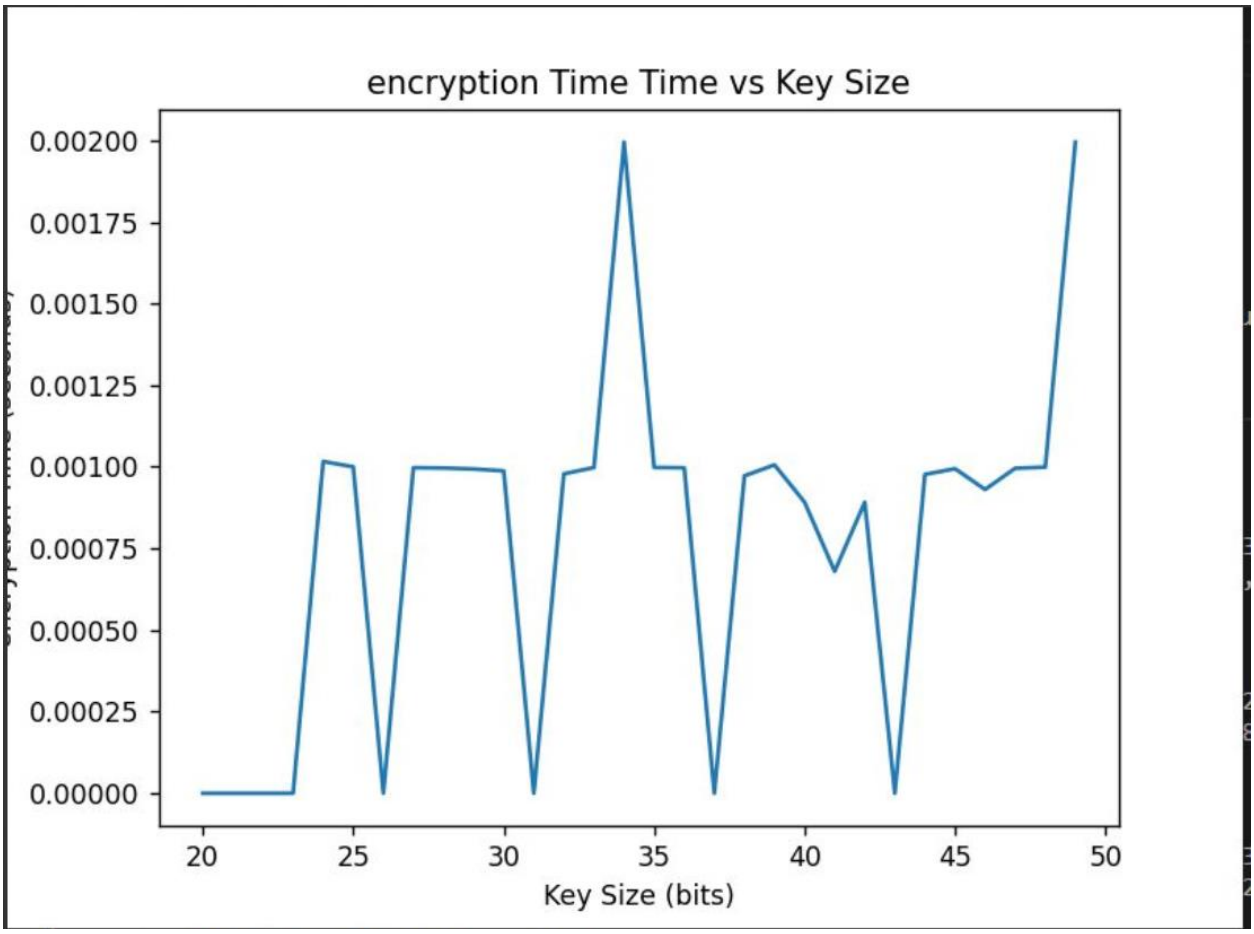


It's a brute force attack we try different key sizes (n) so try different public key sizes from 20 to 30 and for each key size entered the attack see the public key on the channel (in the code it is a thread wake up when user entire his n bits and take his public key).

And I made 2 arrays 1->key sizes 2-> time require for attack.

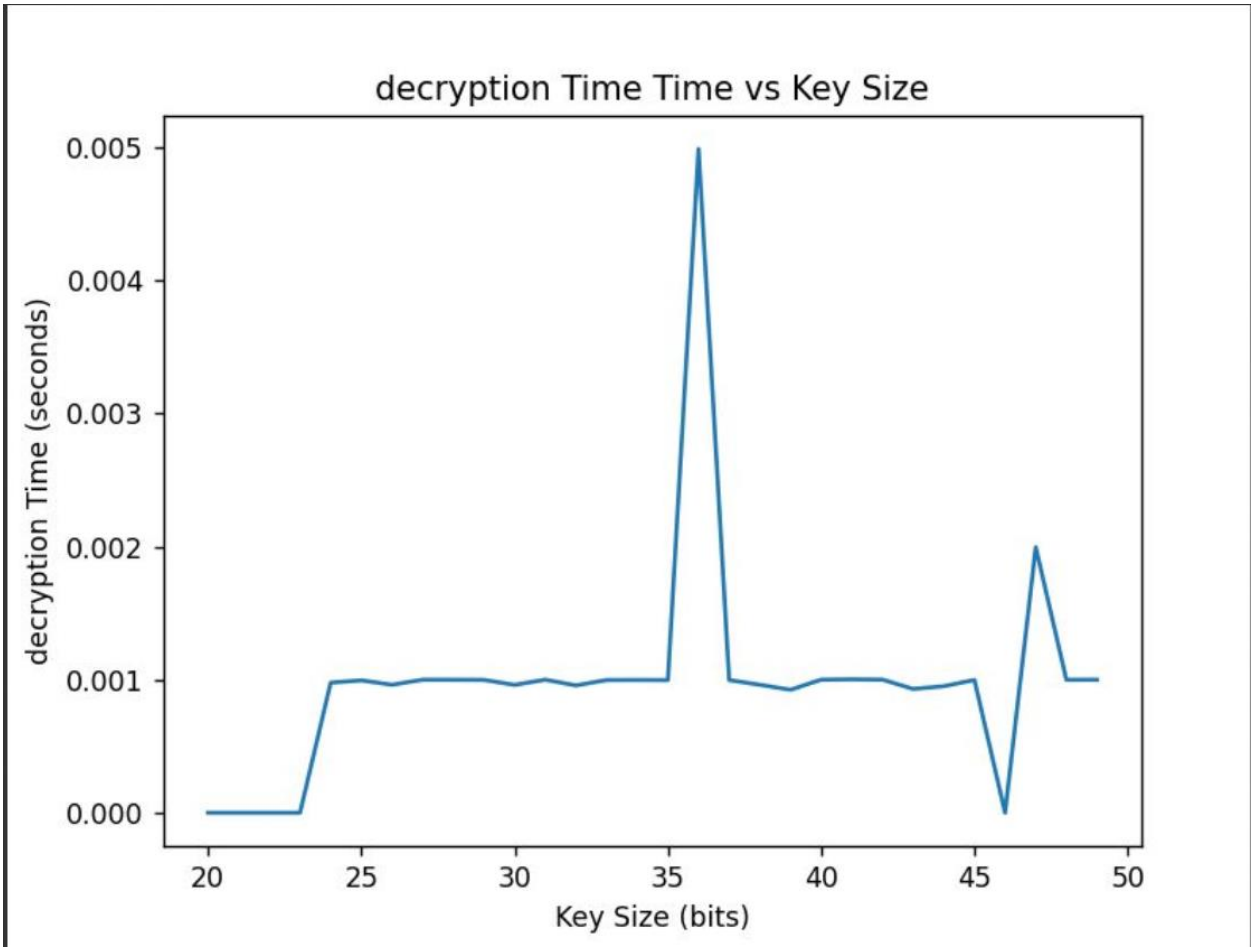
You will notice that the curve is clearly exponential which is the known time complexity of attack (prime factorization)

encryption Time vs Key Size



As we see the encryption is very speed and has nearly **zero** time for this the RSA algorithm is very efficient for encryption

decryption Time vs Key Size



As we see the decryption is very speed and has nearly **zero** time for this the RSA algorithm is very efficient for decryption

Conclusion

1. RSA is a very efficient algorithm for encryption and decryption.
2. RSA is a very efficient algorithm for chatting as you need the speed for real time applications like chatting.
3. Attacking with brute force takes an exponential time.