RSA Assignment

Name: Mohamed Kamal Mohamed Othman

Section: 2

B.N.: 18

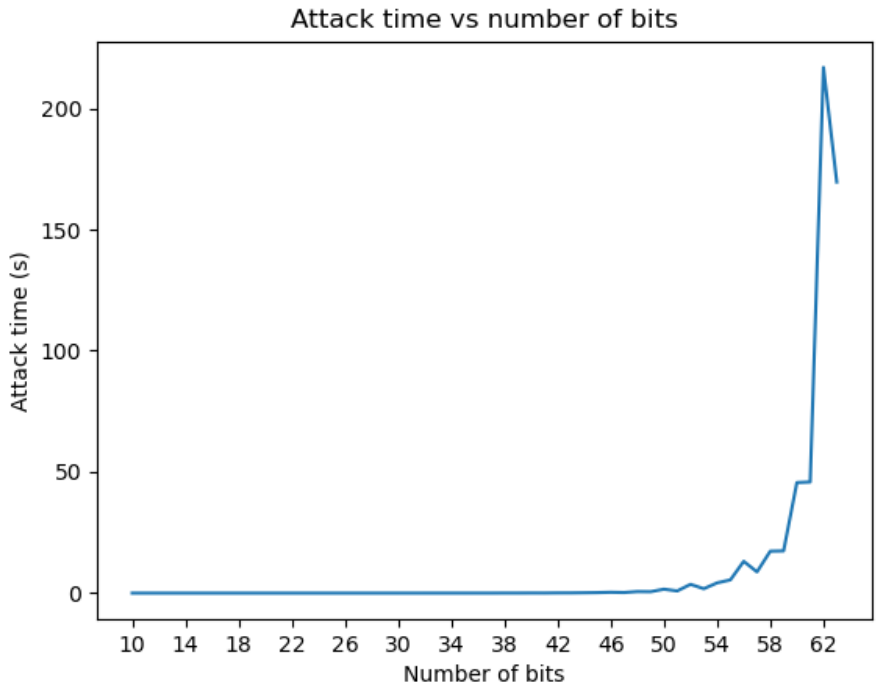
Introduction

The program is divided into two parts: chatting and analysis. The chatting program is used to send and receive encrypted messages. The analysis program is used to perform analysis on how the number of bits (Key size) affect the key breaking process using two methods which are **Prime Factorization** and **Brute force.** The analysis program also shows the time taken to encrypt and decrypt the message as well.

Results and Conclusions

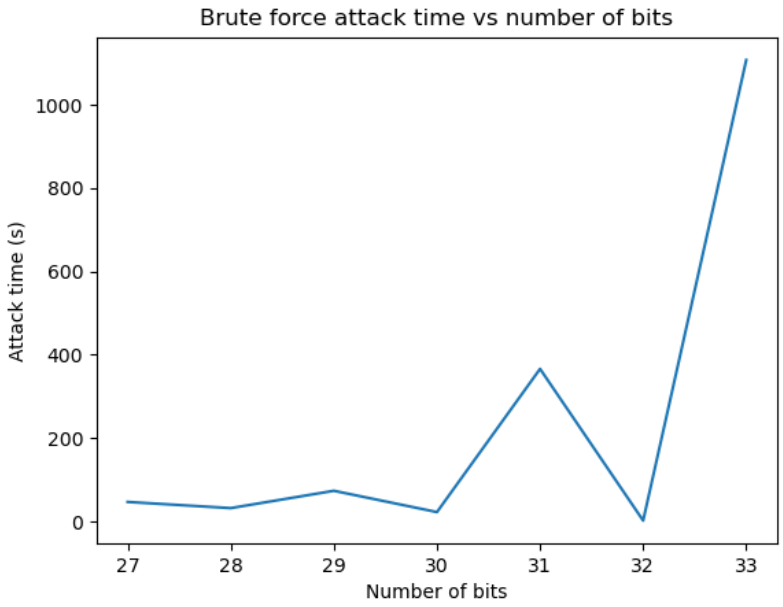
The analysis shows that the time taken to break the key **increases exponentially** with the increase in the number of bits.

The following graph shows the time taken to break the key using prime factorization method:



Note: When using number of bits below 27 bits is presented only for comparison but the message will not be encrypted correctly because the key will be too small to encrypt the message.

The following graph shows the time taken to break the key using brute force method:



We can deduce that the time taken to break the key using prime factorization method is much lower than the time taken to break the key using brute force method. This is because the prime factorization search space ($2^{(number\ of\ bits)/2}$) is much smaller than the brute force search space ($2^{(number\ of\ bits)\ -\ 1}$). Also, the prime factorization search space is limited to the number of primes less than the key which can be used as an optimization. The brute force search space is limited to the number of possible keys.

Both the encryption and decryption time **increases exponentially** because the time taken to encrypt and decrypt the message is directly proportional to the number of bits in the key.

The following graph shows the time taken to encrypt and decrypt the message: