Cairo University
Faculty of Engineering

Department of Computer Engineering

Cryptography

RSA Encryption

Submitted to

Eng. Khaled Moataz

Submitted by

Zeyad Tarek Khairy

Sec: 1

BN: 28

Code: 9202588

Introduction

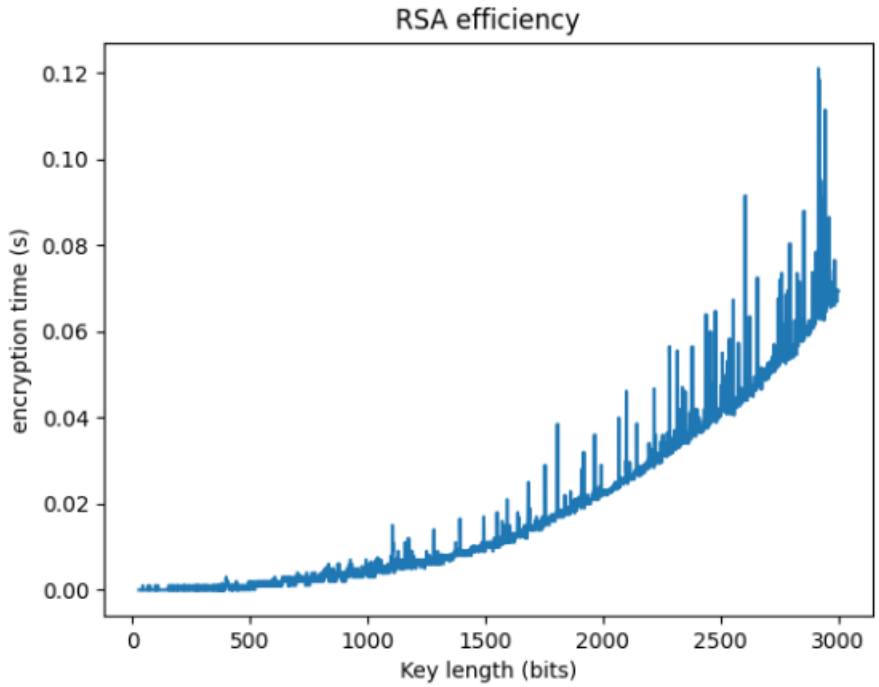
RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission.

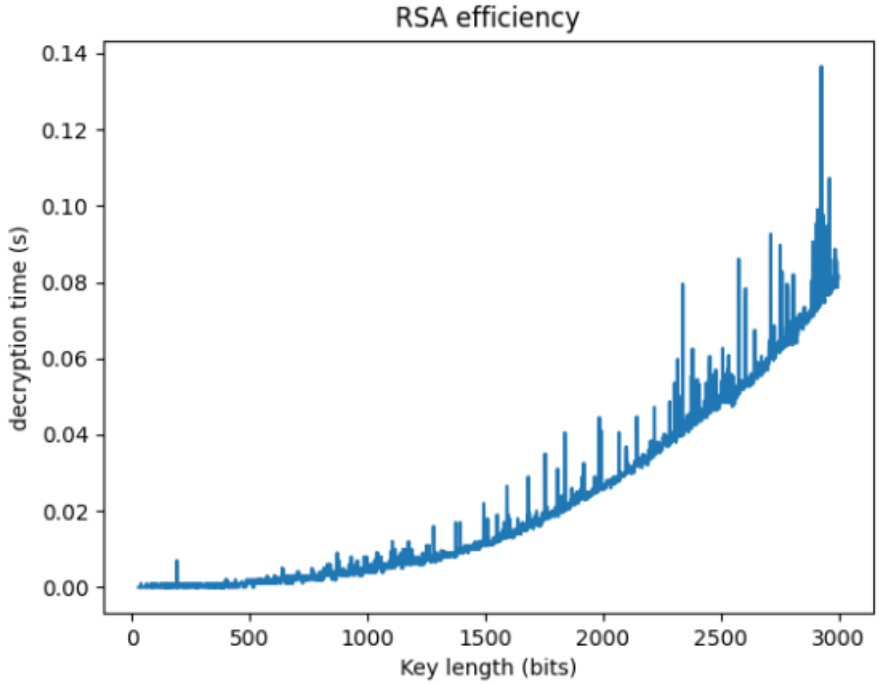
In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret.

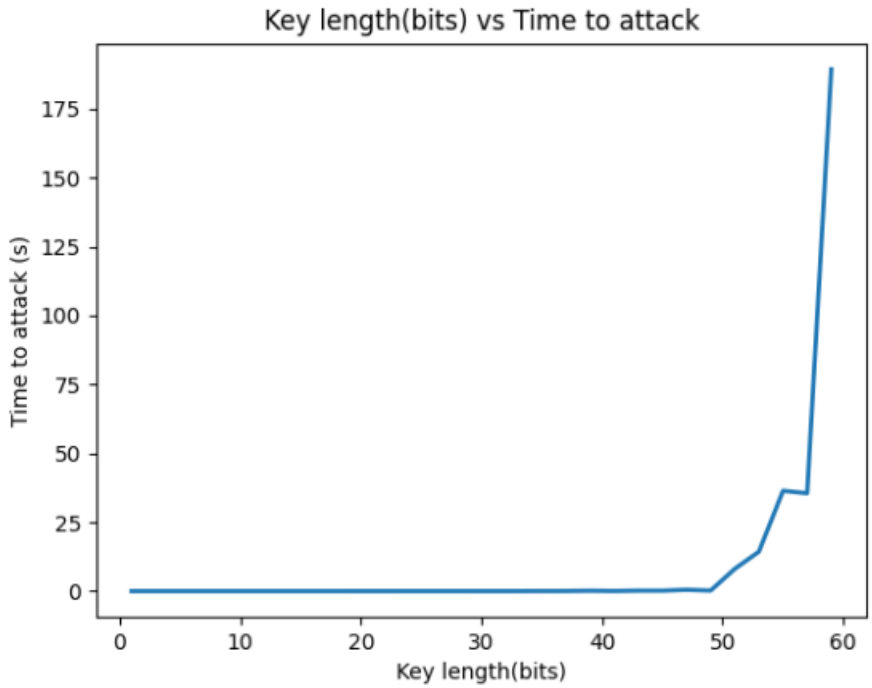
Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". There are no published methods to defeat the system if a large enough key is used.

Screenshots







The implemented algorithm for breaking RSA encryption may experience issues when the number of bits exceeds 64. In such cases, the program may take an exponentially longer time to output the result. This is due to the limitations of the algorithm and the resources available for the program to perform the factorization process. As the number of bits increases, the time required for factorization grows exponentially, making it impractical to break RSA encryption with large key sizes.