Cryptography Assignment 1

Ziad Sherif Muhammed

Sec:1

BN:27

Code: 9202586

RSA

Introduction

The RSA public-key cryptosystem is an important cryptographic tool that is widely used to secure data transmission over the internet. It is considered one of the most secure public-key cryptosystems available, and its security relies on the difficulty of factoring large prime numbers. In this project, we aim to understand how RSA works and its security implications. We built a program that can encrypt/decrypt text using RSA and another program that tries to break RSA and obtain the private key. We also analyzed the impact of different key sizes on the speed of encryption/decryption and the time required to break the algorithm.

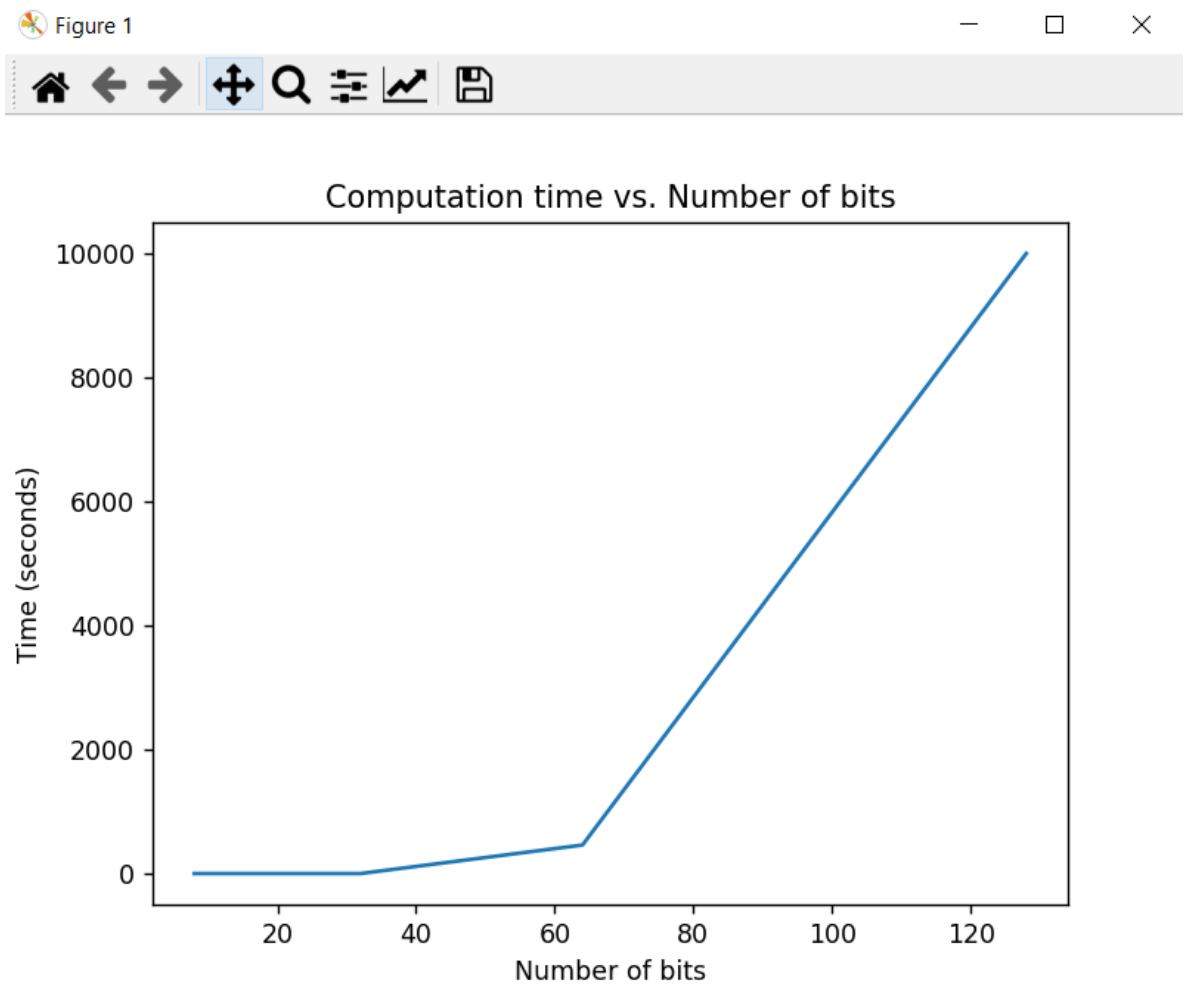
Implementation

Here are some general steps that can help guide the implementation process:

1. Generate two large prime numbers, p and q, and calculate their product n = p * q.
2. Calculate Euler's totient function of n, ϕ(n) = (p - 1) * (q - 1).
3. Choose an integer e such that 1 < e < ϕ(n) and e is coprime to ϕ(n) (i.e., their greatest common divisor is 1).
4. Calculate the private key d such that d * e ≡ 1 (mod ϕ(n)). This can be done using the extended Euclidean algorithm.
5. The public key is (n, e), and the private key is (n, d).
6. To encrypt a message M, convert it to a number m using the character conversion scheme provided in the assignment description. Then, compute the ciphertext C as C = m^e (mod n).

7. To decrypt a ciphertext C, compute the plaintext M as M = C^d (mod n), and then convert it back to characters using the decoding scheme provided in the assignment description.

Screenshots



Notes:

1. It is important to mention that the implemented algorithm for breaking RSA encryption may experience issues when the number of bits exceeds 64. In such cases, the program may get stuck and give an infinite 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.

2. It is important to mention that during testing, the encryption and decryption functions were found to be very fast, with negligible time taken to perform these operations.