Jaypee Institute of Information Technology,
Sector-128, Noida

Information Security Lab,
End Term Project

Topic- Encryption using RSA algorithm and Keyword Cipher

Submitted by:

Divya Shikhar Chauhan 9919103021

Shubh Gupta 9919103022

Submitted to:

Himanshu Agrawal
(Department of CSE & IT, JIIT-128)

December 2021

Problem Statement

Communicating through the internet is very common nowadays. With increased use of this technology, security has also become an important part of it. Cyber-Security makes sure that your information, though it is on a public platform and is accessible to everyone yet it is safe and is visible to people who are under your discretion.

In this project we have tried to encrypt a particular information and then decrypt it using a combination of two encryption algorithms i.e. **RSA encryption algorithm** and **Keyword cipher.**

Let's proceed in the report for the implementation of both.

Introduction

RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

RSA involves a public key and private key. The public key can be known to everyone- it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The private key needs to be kept secret. Calculating the private key from the public key is very difficult.

Some Fields Using RSA Encryption

- *Banking*
    - RSA algorithm is commonly used by banks to protect their data, like customer information and transaction record. Some scenarios are credit card and office computers.
- *Telecommunications*
    - RSA algorithm is useful to encrypt the call data as a concern for privacy issues.
- *Ecommerce*
    - RSA algorithm is useful in protecting user identity for transactions.

Working

Algorithm

The RSA algorithm holds the following features −

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

You will have to go through the following steps to work on RSA algorithm −

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown −

$$N=p*q$$

Here, let N be the specified large number.

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1)*(q-1). The primary condition will be that there should be no common factor of e and totient [i.e (p-1)*(q-1)] except 1.

Step 3: Public key

The specified pair of numbers n and e forms the RSA public key and it is made public.

Step 4: Private Key

Private Key d is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows −

$$ed \equiv 1 \bmod (p-1)(q-1)$$

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula

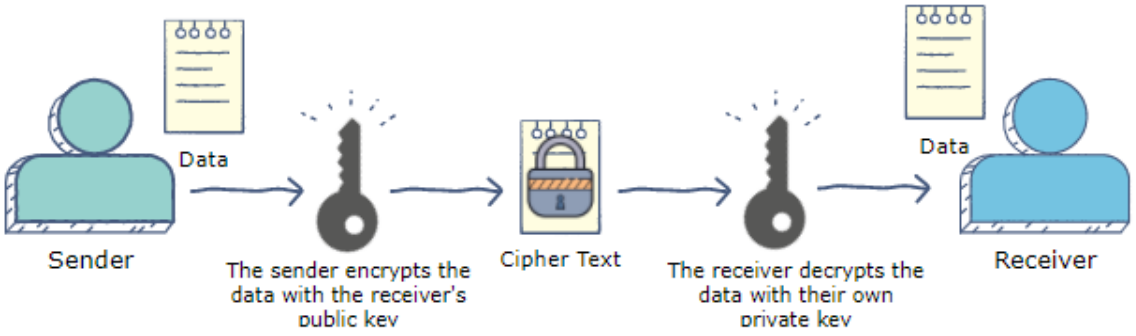
Consider a sender who sends the plain text message to someone whose public key is (n,e). To encrypt the plain text message in the given scenario, use the following syntax −

C = (P^e) mod n

Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver C has the private key d, the result modulus will be calculated as −

Plaintext = (C^d) mod n



Project Description

To send a message using a Symmetric Key encryption, the key needs to be encrypted as well to protect the data. To do so, we used an Asymmetric Key algorithm called RSA encryption technique.

Code-

```
int gcd(int a, int b)                                  //Finds the HCF of e and phi
{⟷}

int find_d(int e, int phi)                        //Finds d such that (d*e) % phi = 1
{⟷}

void string_to_ascii(string a)                          //Converts string to ascii
{⟷}

string ascii_to_string()                                //Converts ascii to string
{⟷}

string encoder(string key)                  //Generates encoded string for KW Cipher
{⟷}

string kwc_encrypt(string msg, string encoded) //Encryption using Keyword Cipher
{⟷}

string kwc_decrypt(string ct, string encoded)  //Decryption using Keyword Cipher
{⟷}

int cdn( int c, int d, int n )                              // works out c^d mod n
{⟷}

int main()                                                          // Driver Code
{⟷}
```

Output

```
Plaintext : Prepare For War. Approaching from North-West.

Original Key:   Secret

Ciphered Text : MOTMSOT ALO WSO. SMMOLSCDFKB AOLJ KLOQD-WTPQ.

*********
RSA Values:

p = 13
q = 11
n = pq = 143
phi = 120
e = 7
d = 103
*********

Encrypted Key:   8 62 44 49 62 129
             :   >,1>ü

Decrypted Key:   83 101 99 114 101 116
             :   Secret

Deciphered Text: PREPARE FOR WAR. APPROACHING FROM NORTH-WEST.
PS D:\Downloads D-Drive>
```

References

[1] https://simple.wikipedia.org/wiki/RSA_algorithm#:~:text=RSA%20

[2] https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

[3] https://www.comparitech.com/blog/information-security/rsa-encryption/

[4] https://brilliant.org/wiki/rsa-encryption/