Ahsanullah University of Science and Technology

Department of Computer Science & Engineering

Course Name: Data Communication

Course No: CSE3211

Assignment

Cryptography & RSA Algorithm

Submitted by

Name : S. M. Tasnimul Hasan Samit

ID : 18.02.04.142

Semester : 3.2

Section : B

Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden. It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as ciphertext and then back again upon arrival. In addition, cryptography also covers the obfuscation of information in images using techniques such as microdots or merging. Ancient Egyptians were known to use these methods in complex hieroglyphics, and Roman Emperor Julius Caesar is credited with using one of the first modern ciphers.

When transmitting electronic data, the most common use of cryptography is to encrypt and decrypt email and other plain-text messages. The simplest method uses the symmetric or "secret key" system. Here, data is encrypted using a secret key, and then both the encoded message and secret key are sent to the recipient for decryption. The problem? If the message is intercepted, a third party has everything they need to decrypt and read the message. To address this issue, cryptologists devised the asymmetric or "public key" system. In this case, every user has two keys: one public and one private. Senders request the public key of their intended recipient, encrypt the message and send it along. When the message arrives, only the recipient's private key will decode it — meaning theft is of no use without the corresponding private key.

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e., Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private. An example of asymmetric cryptography:

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client’s public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So, if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Applications of Cryptography

Digital Currency

A much-known application of cryptography is digital currency wherein cryptocurrencies are traded over the internet. Top cryptocurrencies like Bitcoin, Ethereum, and Ripple have been developed and traded over time. With cashless economies emerging, digital currencies have grabbed the attention of the world. Unregulated by any government or banks, cryptocurrencies are our upcoming future. Blockchain technology has a lot to do with this application. Several nodes in the blockchain are empowered with cryptography that enables the secure trade of a cryptocurrency in a digital ledger system. These ledgers are protected, preserved, and cannot be accessed by any other person or organization.

E-commerce

With the current pandemic shackling us to our homes, the rise of e-commerce has been tremendous. Well, who wouldn't like to enjoy the comfort of shopping in your living room and receiving your hampers the next morning?

However, there's something we should know about e-commerce in order to understand how it works. E-commerce startups enable us to shop items online and pay for them online.

These transactions are encrypted and perhaps cannot be altered by any third party. Moreover, the passwords we set for such sites are also protected under keys to ensure that no hacker gets access to our e-commerce details for harmful purposes.

Military Operations

The applications of cryptography in the military are well-known. Military operations have also derived great use from cryptography for a long time. Used for encrypting military communication channels, military encryption devices convert the real communication characters so that the enemies cannot come to know about their upcoming plans.

Simply put, cryptography safely transmits messages from one end to the other without letting the enemy forces intercept the real meaning. This is a very important application of cryptology as it can be of both public and private use.

On the large scale, it can be widely used for declaring wars and sending crucial messages without the involvement of a messenger. Unlike traditional times, this technology can be precisely used to enhance the military strength of a nation.

RSA Algorithm

```
#include<bits/stdc++.h>
using namespace std;

int x, y, n, t, i, flag;
long int e[50], d[50], temp[50], j;
char en[50], m[50];
string msg;
int prime(long int);
void encryption_key();
long int cd(long int);
void encrypt();
void decrypt();

int main()
{
  cout << "\nEnter two prime numbers : ";
  cin >> x >> y;
   getchar();

  cout << "\nEnter Message : \n";
  getline(cin,msg);

  for(i = 0; msg[i] != NULL; i++)
    m[i] = msg[i];
  n = x * y;
  t = (x - 1) * (y - 1);

  encryption_key();

  cout<<"Public Key : ("<<e[1]<<", "<<n<<")\n";
  cout<<"Private Key : ("<<d[1]<<", "<<n<<")";

  encrypt();
  decrypt();
  return 0;
}

int prime(long int pr)
{
  int i;
  j = sqrt(pr);
  for(i = 2; i <= j; i++)
  {
    if(pr % i == 0)
      return 0;
  }
  return 1;
 }

void encryption_key()
{
  int k;
  k = 0;
  for(i = 2; i < t; i++)
  {
    if(t % i == 0)
      continue;
    flag = prime(i);
    if(flag == 1 && i != x && i != y)
    {
      e[k] = i;
      flag = cd(e[k]);
      if(flag > 0)
      {
        d[k] = flag;
        k++;
      }
      if(k == 99)
      break;
    }
  }
}

long int cd(long int a)
{
  long int k = 1;
  while(1)
  {
    k = k + t;
    if(k % a == 0)
      return(k/a);
  }
}

void encrypt()
{
  long int pt, ct, key = e[0], k, len;
  i = 0;
  len = msg.size();

  while(i != len)
  {
    pt = m[i];
    pt = pt - 96;
    k = 1;
    for(j = 0; j < key; j++)
    {
      k = k * pt;
      k = k % n;
    }
    temp[i] = k;
    ct= k + 96;
    en[i] = ct;
    i++;
  }
  en[i] = -1;
  cout << "\n\nAfter Encryption : \n";
  for(i=0; en[i] != -1; i++)
    cout << en[i];
}

void decrypt()
{
  long int pt, ct, key = d[0], k;
  i = 0;
  while(en[i] != -1)
  {
    ct = temp[i];
    k = 1;
    for(j = 0; j < key; j++)
    {
      k = k * ct;
      k = k % n;
    }
    pt = k + 96;
    m[i] = pt;
    i++;
  }
  m[i] = -1;
  cout << "\n\nAfter Decryption : \n";
  for(i = 0; m[i] != -1; i++)
    cout << m[i];

 cout << endl;
}
```