A RSA algorithm simulation method using C language

Zhenyu Wang[1,*],Siting Wu[2]
[1]Department of Computer Science and Technology
Xi'an University of posts and Telecommunications
710121, Xi'an, CHINA
*Author:ruangongwwk@163.com

Zhuangzhuang Gu[1]
[2]Department of Communications and Information Engineering
Xi'an University of Posts and Telecommunications
710121, Xi'an, CHINA

***Abstract*—In order to solve the problem that data leakage is existed in the Internet era, this paper uses RSA algorithm to encrypt data. First, the basic concepts of cryptography are proposed, and then the basic principles of the RSA algorithm are given. This paper uses C language to simulate RSA algorithm and C/S structure to realize ciphertext transmission. Experimental results show that the RSA algorithm can be used to encrypt data.**

Keywords-RSA algorithm; C language; C/S structure.

I. INTRODUCTION

Information security has become a common topic in society, and cryptography is closely related to cybersecurity, national political security, economic security, social stability and people's daily lives. The information leakage and network crash events have occurred frequently in recnet years. For instance, the "Eternal Blue" event that took place in 2017 is the most impressed event. In this event, the tool developed by the attacker uses the SMB vulnerability of the Windows system to obtain the highest authority of the system. Meanwhile, the criminals created the wannacry ransom virus through the transformation of the tool, which causes large crash in a number of intra-university networks, large intranets and government agencies in Europe and China. In 2013, Alipay has a large-scale data leakage with a total leak of 15 million to 25 million, and the data is used in Internet marketin. The enterprises involved in this incident include Jingdong, Alipay and Dangdang, among which Dangdang has reported to the local public security. Therefore, it's necessary to use efficient encryption algorithm.

Many scholoars at home and abroad have conducted research on data encryption technology. Zhang Shuai et al [1] proposed a watermarking algorithm based on image information entropy theory, and analyzed the extraction process of linear weight selection based on information entropy and the performance of the algorithm. Based on the analysis of the fundamental principles of the RSA algorithm, Li Jinhe [2] programmed the RSA algorithm to encrypt Tibetan characters, and proved the practicability and correctness of the RSA algorithm for Tibetan characters; He Anping[3] proposed a data path based on asynchronous micro-pipeline as a chip design method eliminating the system clock circuit, and designed a suitable asynchronous control framework to construct a fully asynchronous RSA cipher chip.

978-1-7281-3584-7/19/$31.00 ©2019 IEEE

The RSA encryption algorithm based on C language and the process of encryption and decryption are simulated in this paper. Then, the information transmission between different computers by setting up C/S architecture is devekoped.

II. PRELININARY

A. Conception of Cryptography

Cryptography is an ancient science, which generated from the war in human society, and gradually formed an independent discipline. The basic idea of cryptography is to disguise information so that unauthorized persons cannot understand the true meaning of the message. Camouflage is a set of reversible digital transformation of information. The original information before masquerading is called plaintext, and the masqueraded information is called ciphertex. The process of masquerading is called encryption, which is performed under the control of a secret key. A set of mathematical transformations used to encrypt data is called an encryption algorithm.

A cryptosystem usually consisting of the following elements:

(1) M:Plaintext space, which means a finite set of all possible plaintext components.

(2) C:Cipertext space, which represents a finite set of all possible ciphertext components.

(3) K:Key space, which expressed finite set representing all possible key combinations.

(4) E:Encryption algorithm collection, which is a family of encrypted transformations from M to C.

(5) D:Decryption algorithm collection, which is a family of decrypted transformations from C to M.

B. RSA algorithm

The famous public key cryptosystem RSA algorithm is proposed by three-digit scientists of American MIT R.Rivest, A.Shamir and L.Adleman in 1978[4-5]. The algorithm encrypts the message by multiplying the product of two large prime numbers as the public key of the algorithm, and the decryption of the ciphertext must know the corresponding two large prime numbers.

Two large prime numbers p and q are independently selected and calculated to generate the public and private keys:

$$n = p \times q$$

$$\varphi(n) = (p-1) \times (q-1)$$

Here, the Euler function of n is the number of positive integers smaller than n and complementary to each other.

Randomly choosing an intenger which satisfies $1 < e < \varphi(n)$ and coprime with $\varphi(n)$, and then calculating the multiplicative inverse $d = e^{-1} \bmod \varphi(n)$.

Three parameters n, e, d are obtained from p and q. In the RSA algorithm, n and e are used as public keys, and d is used as a private key. The specific encryption/decryption process is shown as follows:

(1) Encryption transformation:First, the plaintext message to be delivered is digitized according to the rule, and then the digitized plaintext is subjected to the following encryption transformation to obtain the ciphertext c:

$$c = c^d \bmod n$$

(2) Decryption transformation:

$$c = c^d \bmod n$$

An instance is proposed to describe the algorithm. If p=5,q=11, the n=55, $\varphi(n)$ =40, and plaintext grouping should be taken as an integer from 1 to 54. According to the above operation rule, the value of the public key e can be calculated as 7, and the value of the private key d is 23. Let the plaintext message be m=53197, and perform the numerical operation on the plaintext according to the grouping method, so m1=53, m2=19, and m3=7. Grouping encryption operations can be obtained:

$$c_1 = m^e{}_1 \bmod n = 53^7 \bmod 55 = 37$$

$$c_2 = m^e{}_2 \bmod n = 19^7 \bmod 55 = 24$$

$$c_3 = m^e{}_3 \bmod n = 7^7 \bmod 55 = 28$$

The decryption of the ciphertext is:

$$c^d{}_1 \bmod n = 37^{23} \bmod 55 = 53 = m_1$$

$$c^d{}_2 \bmod n = 24^{23} \bmod 55 = 19 = m_2$$

$$c^d{}_3 \bmod n = 28^{23} \bmod 55 = 7 = m_3$$

Finally, the plaintext is restored according to the grouping method m=53197.

C. C/S structure and network communication

C/S is a common way in Internet, which refers to two application processes in network communication. The client runs after being called by the user, and actively sends a request to the remote server during communication; the server is a program specially provided for services, and can simultaneously process requests of multiple remote users.

A special Application Programming Interface called socket should be used to relize the communication between client and server. Socket is a basic operation unit which supports network communication with TCP/IP protocol. Network communication using sockets can usually be divided into three phases.

(1)Estabishing the connection

When the socket is created, its port number and IP address are empty, so the application process should call the bind command to get the local address of the socket. Meanwhile, after the server side calls bind, the system must also call the listening command to set the socket to passive mode, so that the system can accept the client's service request at any time. Then, the server calls accept to extract the connection request from the remote client process. One of the variables of the accept command is to indicate from which socket the connection was initiated.

(2)Sending data

Both the client and the server use the send system call command to transfer data on the TCP connection, and use the recv system call command to receive data. Under normal circumstances, the client uses sending command to send the request, and the server uses sending command to send the answer; the server uses recv command to receive the request sent by the client with the sending command, and the client uses the recv command to recive the answer after sending the request.

(3)Connection release

Once the client or server finishes using the socket, the system needs to undo the socket, then call close command to release the connection and undo the socket.

III. ALGORITHM IMPLEMENTATION

The RSA algorithm is simulated with C language and the message is transformed with C/S structure in this paper. The plaintext is inputed by users in client, and ciphertext is obtained from encryption algorithm. Then, the ciphertext is transformed to the server with socket. After receiving the ciphertext, the server decrypts the decryption algorithm and restores it to plaintext. Due to space limitations, only the algorithm code for the key functions is given below.

The encryption algorithm is described Algorithm 1. This function has a total of 7 parameters, in which m represents the plaintext array, and c represents the ciphertext array. The prim function is used to judge the whether a data is coprime with another data, and obtain the public key E. The function private_key takes the values of the public key and the Euler function as input, and outputs the private key D. Since C programs generate overflow and error when computing large data, so the indirect forced type conversion and rounding are used to achieve the remainder in the process of calculating ciphertext.

Algorithm 1

```
void RSA_code(char m[20],int p,int q,int cnt,int c[20],int* E1,int* N1){
```

```
    int N;
    int euler;
    int E;//pubic key
    int D;//private key
    int i;
    N=p*q;
    *N1=N;
    euler=(p-1)*(q-1);
    for (i=2;i<20;i++)
        if (prime(i,euler)==1)
        {
         E=i;
        break;
        }
     *E1=E;
     D=private_key (E,euler);
    for(i=0;i<cnt;i++)
        c[i]=(int)(pow(m[i]-97,D)-
              floor(pow(m[i]-97,D) /N)*N);
}
```

The decryption algorithm is described in Algorithm 2. The algorithm takes ciphertext, public key, and modulus index as input, and outputs the plaintext obtained after decryption.

Algorithm 2

```
void RSA_encode(int c[20],int E1,int N1,int cnt)
{
        int i;
        int decode[20];
        char m_decode[20];
        for(i=0;i<cnt;i++)
 decode[i]=(int)(pow(c[i],E1)-floor(pow(c[i],E1)/N1)*N1);
         for(i=0;i<cnt;i++)
            printf("%d ",decode[i]);
         for(i=0;i<cnt;i++)
            m_decode[i]=decode[i]+97;
         for(i=0;i<cnt;i++)
            printf("%c ",m_decode[i]);
}
```

The algorithm for getting public key is shown in Algorithm 3

Algorithm 3

```
int prime(int n,int euler)
{
        int a[20];
        int b[20];
        int c[20];
        int i;
        int cnt_a=0;
        int cnt_b=0;
        int cnt_c=0;

    for(i=1;i<=n;i++)
                if(n%i==0)
                        a[cnt_a++]=i;
        for(i=1;i<=euler;i++)
                if(n%i==0)
                        b[cnt_b++]=i;

        for(i=0;i<cnt_a;i++)
                if(euler%a[i]==0)
                        c[cnt_c++]=a[i];

        if(cnt_c==1)
                        return 1;
        else
                        return 0;
}
```

IV. EXPERIMENT

This paper implements the simulation of RSA algorithm based on C language, and uses two computers for information transmission. The configuration is shown in TABLE I.

TABLE I. CONFIGURATION OF COMPUTER

Operation system	Windows 7/10
Operating environment	Microsoft Visual C++
Host configuration	Inter Core i5-2430 2.4GHz

In the experiment, first closing the firewall between the two computers and ensuring that the two computers are in the same LAN. In addition,starting the server first in order to receive the ciphertext.

Here, 3 and 11 are selected as two prime numbers. The plaintext “bcd” is inputed on the client, and the ciphertext obtained after encryption is 1, 29 and 9, as shown in Figure 2; the ciphertext is received by the server, and the decryption algorithm is used to recover the ciphertext to the plaintext.

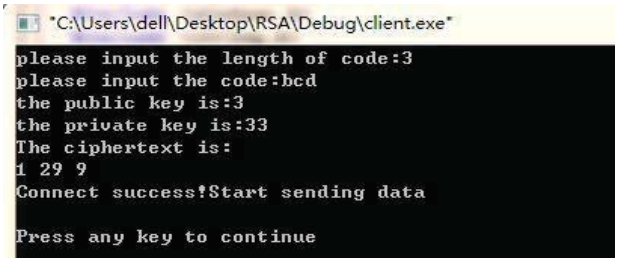

Figure 1. Client sends the ciphertext

V. CONCLUSION

This paper implements the simulation of RSA algorithm based on C language. Firstly, the principle and process of RSA algorithm are given. Then, C/S is used to realize encryption, decryption and ciphertext information transmission. The experimental results show that the encryption and decryption of plaintext can be realized.

In the future research, the following directions will be further explored: (1)The visualization interface should be added to the system in order to enhance human-computer interaction; (2)The numerical methods of plaintext information should be studied, and reasonable mapping rules shoule be given; (3)Implementing more complicated and secure algorithms to implement encryption and decryption process.

Figure 2. Serverreceives the ciphertext

ACKNOWLEDGMENT

This paper is supported by the Graduate Innovation Fund in Xi'an University of Posts and Telecommunications under Grant 103-602080002, by the Department of Education Shaanxi Province, China, under Grant 16JK1697, by the Key Research and Development Program of Shaanxi province, under Grant 2017GY-071 , by the Technical Innovation Guidance Special Project of Shaanxi province, under Grant 2017XT-005, by the the Science Research and Development Program of XianYang City.

REFERENCES

[1] Zhang Shuai,Liu Shaoyun,Zhang Weiwei,and Yang Xuexia, "An Entropy-based WaterMarking Algorithm for Chaotic Encrypted Wavelet Transform," Journal of Taiyuan University of Science and Technology, vol.40,issue 3,pp.175-179,2019.

[2] He Anping,Guo Huibo, and Feng Zhihua, "RSA algorithm encryption based on asynchronous circuit design,". Computer Engineer and Design, vol. 40, issue 4, pp.906-913,2019.

[3] Li Jinhe,Gao Dingguo,and Sun Gaixin. "Application of RSA Algorithm in Tibetan Character Encryption," Electronic Technology and Software Engineering, issue 8, pp.254-256,2019.

[4] Fan Jiulun,Zhang Xuefeng,Liu Hongyue,Xie Xie,and Li Hui, Fundamental of Cryptography, Xi'an: Press of Xidian University,2008,pp.77-79.

[5] Luo Shoushan,Chen Ping,Zou Yongzhong,and Liu Lin. Cryptography and information security technology, BeiJing:Press of BeiJing University of Posts and Telecommunications,2009,pp.89-93.