Research and Implementation of RSA Algorithm for Encryption and Decryption

Xin Zhou
Department of Computer Science and Technology
Harbin University of Science and Technology
Harbin, China
zhouxin@hrbust.edu.cn

Xiaofei Tang
Department of Software
Liaoning University of Science and Technology
Anshan, China
tangxiaofei@163.com

***Abstract*—Cryptographic technique is one of the principal means to protect information security. Not only has it to ensure the information confidential, but also provides digital signature, authentication, secret sub-storage, system security and other functions. Therefore, the encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting. Encryption and decryption algorithm's security depends on the algorithm while the internal structure of the rigor of mathematics, it also depends on the key confidentiality. Key in the encryption algorithm has a pivotal position, once the key was leaked, it means that anyone can be in the encryption system to encrypt and decrypt information, it means the encryption algorithm is useless. Therefore, what kind of data you choose to be a key, how to distribute the private key, and how to save both data transmission keys are very important issues in the encryption and decryption algorithm. This paper proposed an implementation of a complete and practical RSA encrypt/decrypt solution based on the study of RSA public key algorithm. In addition, the encrypt procedure and code implementation is provided in details.**

Keywords- RSA algorithm; encryption; decryption

I. INTRODUCTION

Encryption is one of the principal means to grantee the security of sensitive information. It not only provides the mechanisms in information confidentiality, but also functioned with digital signature, authentication, secret sub-keeping, system security and etc. Therefore, the purpose of adopting encryption techniques is to ensure the information's confidentiality, integrity and certainty, prevent information from tampering, forgery and counterfeiting [1].

At present, the best known and most widely used public key system is RSA, which was first proposed in paper "A method for obtaining digital signatures and public-key cryptosystems" by RL Rivest et al. in 1978. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. Its security is based on the difficulty of the large number prime factorization, which is a well-known mathematical problem that has no effective solution [2]. RSA public key cryptosystem is one of the most typical ways that most widely use for public key cryptography in encryption and digital signature standards.

This paper designed a complete and practical RSA encoding solution and provided the analysis on the source codes based on .NET platform.

II. THE RSA CRYPTOSYSTEM

A. Brief Introduction on RSA and Public-key Cryptography[3]

The key feature of public-key cryptosystem is that the encryption and decryption procedure are done with two different keys – public key and private key, and the private key can not be derived from the public key, that enables the publication of the encryption key without the risk of leaking the secrets The most significant approach of public key cryptography algorithm is RSA, which can resist almost all the known passwords attacks so far.

RSA algorithm, which is named after the inventors, is the first algorithm that can be used both for data encryption and digital signatures RSA algorithm's security depends on the difficulty of decomposition of large numbers. In the algorithm, two large prime numbers are used for constructing the public-key and the private-key. It is estimated that the difficulty of guessing the plaintext from signal key and the cipher text equals to that decomposition of the product of two large prime numbers.

RSA algorithm has been used as a possible authentication methods in ISAKMP / Oakley framework. Diffie-Hellman key exchange algorithm is a key component of the framework. In the beginning of a key agreement session, participants communicate by using Diffie-Hellman algorithm and create shared keys which will be used for key agreement protocol of follow-up steps.

In practice, in order to achieve the optimal efficiency, the symmetric key algorithms and public key cryptography algorithms are always combined together. That is using a symmetric key cryptosystem to encrypt the confidential information needed to be sent, while using the RSA asymmetric key cryptosystem to send the DES key. This takes advantages of both the two kinds of cryptography, namely, high-speed DES and RSA key management mechanism which is of convenience and security.

B. The Process of RSA Algorithm

RSA cryptosystem uses the mode n, the smallest non-negative complete the remaining lines of operation, where n is the product of two different primes p and q [4]. RSA algorithm is described as following.

First, the generation procedure of keys is as follows,

1) Randomly generates two primes P and Q of length K / 2 bit ;

2) Calculate the public key publicKey=P*Q; (public Key's length is k-bit)

3)Generate a random encryption key keyE, 2<=keyE<= Φ(n)-1， where GCD(keyE, Φ(n))=1;

This is the necessary and sufficient conditions for solvability of the decryption key keyE * keyD mod Φ(n)=1, Φ(n) is known as the Euler function of n, the value is Φ(n)=(P-1)*(Q-1)

4) Calculate the decryption key, keyD=keyE-1 mod (n) ,keyE-1 is inverse for the decryption key keyD. The formula of the original equation is keyE * keyD mod Φ(n)=1

Now, the public key, encryption key and decryption key are all created.

Then, the process of encryption of the plaintext and decryption of ciphertext is as follows:

1) Encryption: C = MkeyE mod publicKey; where M is plaintext, C is ciphertext.

2) Decryption: M = CkeyD mod publicKey; in which M plaintext, C is ciphertext.

C. TheImplementation of RSACryptosystem

To implement RSA cryptosystem is a rather complex process, which involves the generation of prime numbers, large integer modular arithmetic and other mathematical calculations. In RSA cryptosystem, p and q are large prime numbers. To achieve it, the most important factor is the efficiency in generate large prime numbers.

Normally, probabilistic algorithms are adopted in generate large prime numbers. This should be: p, q are large prime numbers, when seeking primes p and q with the method of factorization, then the difficulty is actually the same as to attack to RSA (the decomposition of large composite number) , it's feasible as to the computer .

In general, probabilistic algorithms do not focus on generating prime numbers, but first randomly generate a large odd number, then determine whether this odd integer is a prime number with probabilistic algorithms (this process is commonly referred to as Primality Test).

D. RSA's Security

RSA's security depends on the difficulty of integer factorization, whether it is equivalent to integer factorization has not been fully proved in theory because there is no evidence providing that to cracking RSA would definitely require for making large numbers factorization. Suppose there is an algorithm not rely on large number factorization, it should be able changed into integer factorization algorithm. Currently, a number of variants RSA algorithms have proven to be equivalent to integer factorization algorithm. Anyway, decomposition of n is the most obvious way to attack. Nowadays, people have been able to decompose more than 140 decimal large prime numbers. Therefore, the module n must be selected to be large enough depending on the specific usage.[5]

E. Digital Signature with RSA Algorithm

Not only can RSA be used for encryption, but also can be used for authentication. Comparing with Hash signature, in public key algorithms, the generated signature key is stored only on the user's computer, so the safety is at a certain level[6].

Digital signature technology of RSA algorithm is actually achieved by a hash function. Digital signature's feature is that it represents the characteristics of the file. If the file changed, the value of the digital signature will change as well. Different files get different digital signatures. One of the most simple hash function is an accumulation of a series of binary codes and taking the last few bits as the value. Hash function is open to both sides of data .

III. SOFTWARE DESIGN

This project adopts hierarchical design. The fundamental level – the RSA algorithm is implemented with C++ in building localized components according to the end user's local OS. Other functions such as file manipulation, data conversion encoding and graphic interface, are achieved with rapid development library functions on virtual machines (In this paper, the C# language on .NET framework is discussed. The calling procedure of local components and the design patterns are almost the same) [7]. In this development mode, the core function is set at the bottom. It can be expanded continuously with the package of components expending by specific situation. Any level of encapsulation can be directly applied to other projects, such as the components for certain form programs, cross-compiler algorithms library to embedded devices. However, each layer needs to rely on all the components of the bottom.

In sum, the upper layer design uses C#, the bottom algorithm uses C++. It can be managed by a Visual Studio solutions, and bring great convenience to debug. The whole project consists of four layers, C++ class library to achieve the core RSA encryption algorithm, DLL components to package the core C++ class library, .Net class for reference DLL and . Net Forms application to achieve file manipulation.

To take the coding overhead into consideration, the software encryption and decryption of data are not strictly comply with RSA standard PKCS#1, but to meet the premised design requirements, it can still achieve encryption and decryption in a simple way.

IV. IMPLEMENTATION OF RSA ENCRYPTION

A. Realization of the Software

This software application interface is shown as Figure 1; source file interface before encryption is shown as Figure 2; encrypted file interface is shown as Figure 3; the decrypted file interface is shown as Figure 4.

Figure 1. Encryption/Decryption application interface

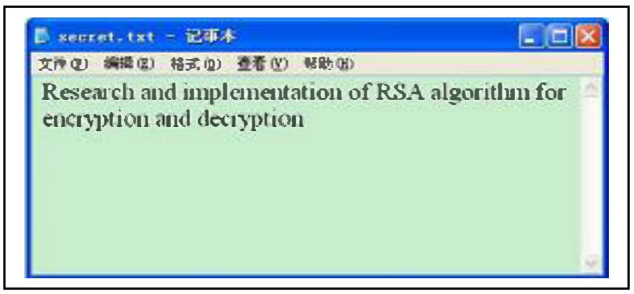

Figure 2. Source file interface

Figure 3. Encrypted file interface

Figure 4. Decrypted file interface

B. Reference Code for Primes Generating Process During Encryption

```
vlong Prime_factory_san::find_prime( vlong & start )
{
 unsigned SS = 1000; // should be enough unless we are unlucky
 char * b = new char[SS]; // bitset of candidate primes
 unsigned tested = 0;
 while (1)
 {
  unsigned i;
  for (i=0;i<SS;i++)
   b[i] = 1;
  for (i=0;i<np;i++)
  {
   unsigned p = pl[i];
   unsigned r = start % vlong(p); // not as fast as it should be - could do with special routine
   if (r) r = p - r;
   // cross off multiples of p
   while ( r < SS )
   {
    b[r] = 0;
    r += p;
   }
  }
  // now test candidates
  for (i=0;i<SS;i++)
  {
   if ( b[i] )
   {
    tested += 1;
    if ( is_probable_prime_san(start) )
     return start;
   }
   start += 1;
  }
 }
 delete [] b;
  }
```

V. CONCLUSION

The encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting. Encryption and decryption algorithm's security depends on the algorithm while the internal structure of the rigor of mathematics, it also depends on the key confidentiality. This paper contains a complete discussion of the cryptography, encryption, decryption, and RSA public key and other related technology applications in the military, business, privacy and other fields of information security which plays an important role. Problem for RSA encryption on the file, it indicates the RSA mathematical algorithms in the computer industry's importance and its shortcomings. It discusses the questions of how to apply to the personal life of RSA information security issues. And also contains the use of RSA and the basic principles of data encryption and decryption. In the end, it proposed a new program to improve RSA algorithm based on RSA cryptography and the extensive application .In summary, this issue of the RSA encryption and decryption keys, RSA algorithm, the new use of the RSA and other issues to study and make some new programs, future work should be in the new RSA cryptographic algorithms and a wide range of applications continue to research.

ACKNOWLEDGMENT

Xin Zhou and Xiaofei Tang thank professor Xinghong Ling of Soochow University for his directive discussion in RSA algorithm study.

REFERENCES

[1] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory, Nov. 1976, 22: 644-654.

[2] R.L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, Feb. 1978, 21(2) : 120-126.

[3] E. F. Brickell, A fast modular multiplication algorithm with application to two-key cryptography, in Proc. CRYPTO'82 Advances Cryptology, Plenum Press, New York and London, 1982: 51-50.

[4] J.-H. Hong, RSA Public Key Crypto-Processor Core Design and Hierarchical System Test Using IEEE 1149 Family, Ph.D. dissertation, Dept. Elect. Eng., National Tsing Hua Univ., Hsinchu, Taiwan R.O.C., 2000: 322-334

[5] Steve Burnett and Stephen Paine, The RSA Security's Official Guide to Cryptography, CA USA: Osborne/McGraw-Hill, 2001.

[6] Dorothy E. Denning, Digital Signature with RSA and Other Public-Key Cryptosystems, Communications of the ACM, 1984.

[7] Ming-Der Shieh, Jun-Hong Chen, A new modular exponentiation architecture for efficient design of RSA cryptosystem, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2008.