Computer and Information Science

www.ccsenet.org/journal.html

Vol. 1, No. 3

August 2008

Study on the Scheme for RSA Iterative Encryption System

Yulian Shang

School of Information and Engineering

Taishan Medical University

Taian 271016, China

Wuyuan Jia

School of Chemistry and Chemical Engineering

Taishan Medical University

Taian 271016, China

Peng Li

School of Information and Engineering

Taishan Medical University

Taian 271016, China

Pengfei Zhu

National Laboratory of Pattern Recognition

Automation Institute of Chinese Sciences Academy

Beijing 100080, China

Abstract

Based on the RSA public key cryptosystem, in this article, we put forward one sort of iterative encryption scheme based on RSA. The multiple keys can make attackers' attacks to the system more difficult and further enhance the security of the key. Through the simulation of software, we realize the encryption transmission of binary image and validate the improvement of the RSA iterative encryption effect.

Keywords: Public key cryptosystem, Iterative encryption system, Key security

1. Introduction

In 1978, Rivest, Shamir and Adleman in MIT put forward the asymmetric key (public key) system which was called the RSA cryptosystem (R. L. Rivest, A. Shamir & L. M. Adleman, 1978, p.20-26). The RSA cryptosystem is one milestone in the developmental history of cryptography, and it is the representative arithmetic of the public key cryptosystem based on big integer decomposability. Because of its simple arithmetic, it is very easily realized in actual application, and it is the most successful cryptography in theory and one of public key system which is most extensively applied at present (Yang, 1999, p.63-66 & Shang, 2004, p.238-242). In the traditional RSA encryption system, we require that the key length has 2048 bits in order to ensure the security of the encryption system, and Lu Changjin and Shi Kaiquan adopted the iterative encryption-decryption arithmetic and obtained better encryption effect (Lu, 2003, p.546-549 & Lu, 2003, p.681-684). In this article, we also put forward the iterative encryption-decryption arithmetic based on the RSA public key cryptography. Because the operations used in this scheme are power arithmetic and modular arithmetic, the complexity of the operation is same to the RSA cryptography. In practice, we can select iterative times properly according to concrete situation. The result of the experiment indicates that the security of the iterative encryption is higher than the security of the single encryption, and the fatalness that the illegal attacker attacks the encryption system is lower and the encryption system is safer.

2. The iterative public key encryption system based on RSA

Based on the RSA public key encryption system, in this article, we put forward an iterative encryption scheme based on RSA to enhance the security of the key. We will concretely introduce the iterative public key encryption system based on RSA and give the structure of this iterative arithmetic (because of the limited length of the article, we only give the

iterative RSA arithmetic with multiple key pairs and the iterative RSA signature arithmetic).

2.1 The RSA iterative encryption arithmetic with multiple key pairs

Supposing: A and B are the two parties of encryption communication, A is the transmitter of information, and B is the receiver of information. Starting from the universality, we suppose that A and B respectively select random t public keys and private keys, the public keys are public, and the private keys are secret, and they are respectively independent each other, and one can not be deducted from the other one. The public information is $m \in M$, and the secret information is c.

For A: Select t pairs of big prime number p, q randomly and compute $n^A = \{n_1^A, n_2^A, \Lambda, n_t^A\}$. The corresponding public key set is $e^A = \{e_1^A, e_2^A, \Lambda, e_t^A\}$, e_i^A is one random public key of A. The corresponding private key set is $d^A = \{d_1^A, d_2^A, \Lambda, d_t^A\}$, d_i^A is one random secret key of A. $i = 1,2,\Lambda, t$.

For B: Select t pairs of big prime number p, q randomly and compute $n^B = \{n_1^B, n_2^B, \Lambda, n_t^B\}$. The corresponding public key set is $e^B = \{e_1^B, e_2^B, \Lambda, e_t^B\}$, e_j^B is one random public key of B. The corresponding private key set is $d^B = \{d_1^B, d_2^B, \Lambda, d_t^B\}$, d_j^B is one random secret key of A. $j = 1,2,\Lambda, t$.

Definition 2.1: Define the public information m, $c_1 = (m^{e_1^B}) \bmod n_1^B$ is the first order encryption of m, $c_i = (c_{i-1}^{e_i^B}) \bmod n_i^B$ is i times iterative encryption of m, where $i \in \{1,2,\Lambda, t\}$.

Definition 2.2: Define $c_t = (c_{t-1}^{e_t^B}) \bmod n_t^B$ is t times iterative encryption of m, and it is also called as the secret information c corresponding with m in the encryption communication.

Definition 2.3: Define the corresponding information c with t times iterative encryption, and $m_1 = (c^{d_t^B}) \bmod n_t^B$ is once decryption of c, $m_j = (m_{j-1}^{d_{t-j+1}^B}) \bmod n_{t-j+1}^B$ is j times decryption of c, where $j \in \{1,2,\Lambda, t\}$.

Definition 2.4: Define $m_t = (m_{t-1}^{d_1^B}) \bmod n_1^B$ is t times decryption of c with t times iterative encryption, i.e. the m produced through decryption.

The process of iterative encryption communication between A and B is described as follows.

A gets m and completes the iterative encryption, and transmit c to B.

Suppose that m is one random public information sect in the public information M which is digitized and grouped, and according to the appointed order, A gets m and encrypt it as c by the public key $e^B = \{e_1^B, e_2^B, \Lambda, e_t^B\}$ of B.

The process of t'th order encryption is:

$$c_1 = (m^{e_1^B}) \bmod n_1^B$$
$$c_2 = (c_1^{e_2^B}) \bmod n_2^B$$
$$\cdots$$
$$c = c_t = (c_{t-1}^{e_t^B}) \bmod n_t^B$$

Where, the expression of the i'th time encryption is $c_i = (c_{i-1}^{e_i^B}) \bmod n_i^B$, c_i is the secret information of m through i times encryption. A transmits c to B. $i \in \{1,2,\Lambda, t\}$.

B receives c and completes the iterative decryption and obtains m.

When B receives c, according the corresponding order, B implements iterative decryption to the secrete information by his own private key, and finally obtains the public information m.

The process of t'th order decryption is:

$$m_1 = (c^{d_t^B}) \bmod n_t^B$$
$$m_2 = (m_1^{d_{t-1}^B}) \bmod n_{t-1}^B$$
$$\cdots$$
$$m = m_t = (m_{t-1}^{d_1^B}) \bmod n_1^B$$

Where, the expression of the j'th time encryption is $m_j = (m_{j-1}^{d_{t-j+1}^B}) \bmod n_{t-j+1}^B$. B decrypts c, obtains the public information m and completes the whole encryption communication. $j \in \{1,2,\Lambda, t\}$.

Obviously, when t=1, the public key of A is e^A, the corresponding private key is d^A, the public key of B is e^B, the corresponding private key is d^B, so the above encryption communication process can be simplified as follows:

A encrypts the public information m to the secret information c and transmits it to B.

$$c = (m^{e^B}) \bmod n^B$$

B decrypts the secret information c to the public information m.

$$m = (c^{d^B}) \bmod n^B$$

The process of encryption communication can be reverted the encryption form in the initial RSA system.

2.2 Arithmetic discussion

(1) As viewed from the encryption-decryption arithmetic, the iterative encryption system based on RSA is still based on the RSA public key cryptography, so its security is still based on the problem of big integer decomposability. Though the arithmetic still uses the iterative arithmetic, but it is the modular arithmetic and power arithmetic, so the complexity of the operation is not be added comparing with RSA cryptography.

(2) In this iterative encryption system based on RSA, because the transmitter A implements iterative encryption to the public information by t public keys $e^B = \{e_1^B, e_2^B, \Lambda, e_t^B\}$, the key attacker can decrypt the secrete information when he obtains all t secrete keys $d^A = \{d_1^A, d_2^A, \Lambda, d_t^A\}$ which is very difficult to be completed, so when B loses one or t-1 keys (i.e. the number of the key which is lost is less than t), the information can not be lost and juggled. Therefore, the key space in the iterative arithmetic increase the randomicity of the key selection, and the order that the iterative encryption selects the key is random, which all can enhance the security of the key.

3. Example analysis and software simulation

In this article, we use the improved encryption scheme to encrypt the image (image element value), select the binary image lean.bmp (256×256) to implement the simulation experiment, and we can see the improvement of encryption effect obviously.

3.1 Software simulation

The experiment of software simulation mainly uses Matlab6.0 to compete the encryption transmission of binary image (the encryption of image element value in fact), and the experiment result includes following aspects which take the image lena.bme as the examples.

The initial image is Figure a, the once encryption-decryption of image are shown in Figure a1 and Figure a2, and the image iterative encryption arithmetic with multiple key pairs are shown in Figure a3 and Figure a4.

3.2 Analysis of experiment result

From above the results of simulation experiment, we can obtain following conclusions.

(1) When the image is implemented encryption-decryption operation every time, it can be resumed to the image before encryption without distortion. We use the data encryption arithmetic to encrypt and transmit the image element values, and its principle is based on the data encryption, but not the direct encryption transmission of the image, which also proves the validity of various encryption-decryption algorithms based on RSA when the image element values are taken as the public information and implemented image encryption arithmetic.

(2) As viewed from the visual effect of image encryption, the iterative encryption (two times) (Figure a3) has better effect than the once encryption (Figure a1), and the image is more disorder which indicated the change of the image element values are larger. Therefore, the system security of the iterative encryption is higher than the system security of the once encryption, and the key of the encryption system is safer.

(3) The improvement of encryption arithmetic based on RSA encryption can be used in the encryption transmission of image, which can implement encryption transmission when the image is not be distorted, and complete the image encryption transmission from another view, and it has very extensive applications in practice.

4. Conclusions

In this article, we put forward the iterative public key encryption system based on RSA, and the practice proves that the RSA iterative encryption system can obtain better encryption effect. However, in this iterative encryption system, large of encryption key set and decryption key set are used, and one important problem that we face is how to manage these enormous key sets and make illegal attackers can not purloin the keys of the encryption communication system, otherwise, there are not effective method to produce randomly big random number to produce the RSA keys.

References

Huang, Yuanfei & Chenlin. (2001). *Information Security and the Core Technology of Encryption and Decryption.* Shanghai: Pudong Electronic Press. p.134-154.

Lu, Changjin & Shi, Kaiquan. (2003). One Dimension Iteration Encryption-recognition of Image. *Journal of Shandong University (Engineering Science).* No. 33(5). p.546-549.

Lu, Changjin & Shi, Kaiquan. (2003). Two Dimension Mixed Iteration Encryption-recognition of Image. *Journal of Shandong University (Engineering Science).* No. 33(6). p.681-684.

R. L. Rivest, A. Shamir & L. M. Adleman. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM.* No.21(2). p.20-26.

Shang, Yulian, Fu, Haiyan & Shi, Kaiquan. (2004). Improved Authentication and Key Distribution for Internet Environment. *Journal of Hainan Normal University (Natural Science).* No. 17(3). p.238-242.

Yang, Zhimin. (1999). Making the Way of RSA Reusing the Public Key to Truth in Computer Information Network. *Journal of Anhui Institute of Architecture & Industry (Natural Science).* No. 7(4). p.63-66.

Figure a. lena.bmp (Initial Image)

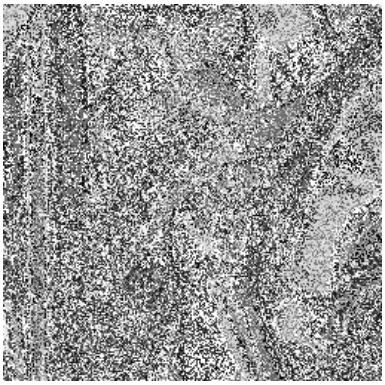

Figure a1. Once Encryption Image

Figure a2. Once Decryption Image

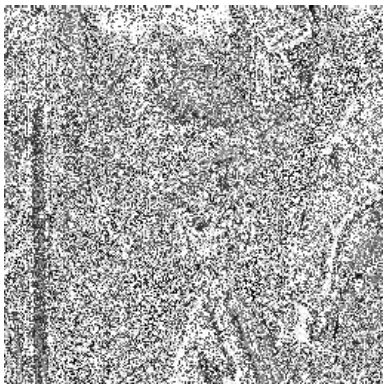

Figure a3. Iterative Encryption Image (Twice)

Figure a4. Iterative Decryption Image