The Principle of RSA Encryption Algorithm and Its Application in Reality

Zhixin Chen

Hangzhou No.4 international high school, Hangzhou 310018, China.

1575530481@qq.com

Abstract

In this passage, we analyzed the RSA encryption algorithm and put forward some improvement methods . Summariesd its practical application in life, respectively through the QR code and smart medicine boxes and other four applications.

Keywords

RSA application.

1. Introduction

RSA [8] public key cryptography was proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. It was first announced in the United States in July 1987, when all three worked as interns at the Massachusetts institute of technology. The RSA is a combination of the first letters of their surnames. RSA is the most influential and commonly used public key cryptography algorithm, which can resist the vast majority of cryptographic attacks known to date, and has been recommended as the public key data encryption standard by ISO.

Today only short RSA keys can be broken by force. As of 2008, there was no reliable way to attack RSA algorithms. As long as the key is long enough, messages encrypted with RSA are virtually unbreakable. However, with the development of distributed computing and quantum computer theory, RSA encryption security has been challenged and questioned.

The RSA algorithm is based on a very simple number theory fact: it is easy to multiply two large primes, but extremely difficult to factor the product, so the product can be exposed as an encryption key.

2. Origin of RSA

2.1 The origin of RSA encryption algorithm

Before talking about RSA principles [9] , there are some basic properties , such as the congruence theorem, prime factorization, Euler functions, and Fermat's theorem.

Multiplicative property: If a≡b(mod m) · c≡d(mod m) · so ac≡bd(mod m) Power operation ：if a≡b(mod m) so (mod m) $a^n \equiv b^n$

Euler functions ：if a,m∈ N · (a,m)=1 · so $a^{\varphi(m)} \equiv 1 \pmod m$

If m is a prime, so φ(m)=m-1

$$\varphi(m = q1^{r^1} \times q2^{r^2} \times \ldots \times qi^{r^3}) = m(1-\frac{1}{q1})(1-\frac{1}{q2})\ldots(1-\frac{1}{qi})$$

Fermat's theorem: if P is prime ,then $a^p \equiv a(\mathrm{mod}\ p)$.

2.2 Talk about the principle of RSA

The firstly we choose two large and different prime Numbers, p and q. Let N be equal to the product of p and q. So we can use Euler functions to get

formula : $\varphi(N)=\varphi(p\times q)=\varphi(p-1)\varphi(q-1)=(p-1)(q-1)$ .Then we assume that ed equal to k product with φ(N) then add 1, also equal to k(p-1)(q-1)+1. So we can get

ed≡1mod φ(m) .So we're going to encode this information into the value a, which have a range between 0 and N-1. Then we set the encryption formula as $a^e \equiv b \bmod N$, the range of b is also between 0 and N-1, and the decryption formula as $b^d \equiv a \bmod N$. If people want to know d ,so they need to know the Euler function φ(n).If they want to know the Euler function φ(n), so they need to know p and q. To know that p and q need to be factored into N.

All in all , the bigger primes p and q that you use, the harder to let enemy to decipher, so the information will be more safety.

2.3 Proof the principle of RSA

Now let's proof this principle, because $a^e \equiv b \bmod N$, so $b^d \equiv a^{ed} \equiv a^{k(p-1)(q-1)+1} \bmod N$. So we just need to show $a^{k(p-1)(q+1)+1} \equiv a \bmod N$. Then we talk about two situations:

If p and a are coprime ,then we can follow the Fermat's theorem, which is $a^{p-1} \equiv 1 \bmod p$, so that $a^{k(p-1)(q-1)} \equiv 1^{k(q-1)} \equiv 1 \bmod p$, then multiply both sides by a, so we can get $a^{k(p-1)(q-1)+1}$ ≡a mod p.

If p and a are not coprime , so p is divisible by a, thus p is divisible by $a^{k(p-1)(q-1)+1}$. So $a^{k(p-1)(q-1)+1} \equiv a \equiv 0 \bmod p$.

From what has been discussed above, whether p is a prime number or not , $a^{k(p-1)(q-1)+1} \equiv a \bmod p$ is always can be done.Then we can deduce a very similar equation $a^{k(p-1)(q-1)+1} \equiv a \bmod q$. So we can be sure that p and q both can divisible $a^{k(p-1)(q-1)+1} - a$.

Because p and q are prime Numbers, so the product of p and q is also divisible $a^{k(p-1)(q-1)+1} - a$, because N equal to product of p and q. So we can proof the principle : $a^{k(p-1)(q-1)+1} \equiv a \bmod N$.

3. The improving of RSA

3.1 Speed of RSA encryption algorithm

Mr. Yang and Mr. Lu [1] studied the encryption speed of RSA encryption algorithm. Some improvements have been made in the operations of large modular power, modular multiplication and square equality. The efficiency of RSA encryption algorithm is improved.

They first described the detailed process of RSA encryption algorithm. It also shows how exponential operation, large number operation, Montgomery modular multiplication operation and large number square operation are improved again. Then it introduces how RSA algorithm is implemented. List the relevant steps separately. The actual test was done in a simulated environment. The test results were calculated by computer and the corresponding table data were given. Finally, the experimental summary was obtained by comparing the data, and they discussed the improvement of several aspects mentioned.

The algorithm to improve RSA is designed and implemented. The efficiency of RSA encryption algorithm is improved, and the acquisition speed of prime Numbers and RSA encryption speed are tested.

3.2 Something about MPI

In real life, there is often a lot of data that needs to be kept secret. RSA encryption algorithm in the complex judgment and large number operations. It takes a lot of time to calculate. The running speed and capacity of the computer and other aspects also have very high requirements.

Mr Lu[2] proposed the application of MPI. He thinks the MPI has enormous numerical and data-processing power. Therefore, he started from RSA encryption calculation and conducted experiments through MPI application to prove that it can improve speed, reduce capacity requirements and improve data security. He begins with a brief description of the RSA encryption algorithm. The MPI

is also introduced. The MPI system is a library of all the messaging functions that have standard interface specifications. Then the advantages of parallel computing environment MPI in parallel processing are illustrated. The message passing system based on MPI is adopted to improve the running speed and security of the algorithm. Two key problems in RSA encryption are described in detail: the selection of coprime and the computation of an inverse. He showed us the detailed flow chart of the algorithm.

Finally, the conclusion is given. MPI provides a convenient programming platform for running parallel programs and user constructs. Through the application of MPI in RSA algorithm, the result is efficient, accurate and safe.

3.3 The Java language

The Java language is an object-oriented programming language with extremely strong security and network processing capabilities. So Mr. Cao and Mr. Li [6] decided to use the RSA encryption algorithm to secure the output of experimental data in a Java environment.

They first introduced the Java security system, Java through its own security mechanism to prevent the production of virus programs and download programs to the local system threat damage. Then the RSA encryption algorithm system is described in detail. By showing the process diagram of encryption and decryption, the realization of RSA algorithm is expressed clearly and concisely.

Finally, they summarizes thier ideas. RSA is the most widely studied public key algorithm, but it has many defects in theory and technology. Therefore, Java can realize based on RSA data encryption transmission on different platforms, and operational and safety are increased than before.

4. The applications of RSA

4.1 Authentication system

Mr. Zhu and Mr.Li [3] proposed an identity authentication system based on RSA encryption algorithm. It is used to identify problems that cannot be separated from accident liability when an accident occurs. The feasibility and safety of the system are also analyzed.

They started by describing the process of Kerberos authentication with examples. Again, to illustrate the shortcomings of the Kerberos authentication method: first, the inability to distinguish between those responsible for accidents. Second, I can't explain the cause of the accident. Third point: third party security sensitivity. The authentication process based on public key encryption is described. The accompanying pictures illustrate the process more clearly. The feasibility, security and efficiency of the algorithm are analyzed. Instead of using data to back up their claims, they gave more practical examples. Through different people's different Angle to carry on the analysis, finally summed up the conclusion.

Based on the defects of this key encryption identity authentication system, an identity authentication system based on RSA is proposed and its performance is analyzed. It also points out that the system is not perfect. In asymmetric encryption, this method is less efficient. Therefore, the advantages and disadvantages should be weighed according to the actual situation.

4.2 QR code

QR code has been widely used because it can store a lot of information and are easy to use. Mr. Li and Mr. Zheng [4] discussed the application of RSA encryption algorithm on QR code. They used asymmetric cryptography RSA encryption algorithm to encrypt and decrypt the data before the generation of QR codes from the perspective of information security.

First, they explained the importance of information security in modern society. Then briefly introduces the composition of QR code and the basic part of RSA algorithm. It also shows that RSA encryption algorithm is applied to the two-dimensional code information security, mainly in the two-dimensional code coding before the data encryption, and then in the verification of the data decryption. Instead of verifying the results with data, they explained each step by derivation. At last they explained their conclusion.

They believe QR codes can be combined with RSA encryption. This can more ensure the security of information, but also can solve the anti-counterfeiting problem.

4.3 Smart medicine boxes

Smart medicine boxes are for home users. It can be a smart device for drug storage, medication management, and remote communication with doctors and manufacturers. Therefore, it contains more private data, such as text data, pictures and videos. If use the same algorithm encryption, it will lead to the encryption strength is not enough, easy to exist security hidden trouble. Therefore, Ms. Chen and Mr. Li [5] proposed to improve RSA encryption algorithm. By adjusting the key length, the security of text data and the encryption speed of large-capacity data are considered.

They first described the use of smart medicine boxes, which can store drugs at different temperatures and can be stored in different categories. Then the data characteristics of the intelligent medicine cabinet are analyzed. The flow of text data is relatively small, generally for permanent data, security and encryption strength are required to be higher. These properties of the picture are also relatively high. However, due to the large flow of video, the security and encryption strength are general, and the storage time is short, but the transmission efficiency is high. They also described the problem of the traditional RSA algorithm, they believe that the traditional algorithm encryption strength and encryption speed produced a contradiction, both can not be the best. Based on this problem, they adjust the key length. The text data is encrypted using a long key. Instead, large data such as video and pictures are encrypted with short keys. In this way, the security of text data and the encryption speed of large-capacity data are taken into account to realize the safe storage of intelligent medicine cabinet. They went on to elaborate on the process of improving RSA. Then three kinds of data before and after the improvement are compared: ciphertext length, encryption time and decryption time. The corresponding table data and analysis are also presented. Finally, they believe that the current problem is that too many users of a single wireless connection affect the stability, and deployment density can also lead to overlapping interference with the same frequency. At the same time, they also proposed several optimization Suggestions, such as layout adjustment, speed limit technology, gate isolation and reasonable frequency planning.

4.4 The smart card

In our daily life, IC card has almost become a necessity for everyone to travel, which can provide us with great convenience. Mr. Tu, Ms. Liu and others [7] discussed the application of RSA encryption algorithm in IC card and the relevant ways to implement RSA algorithm in IC card.

They first introduced the basic steps of RSA encryption algorithm, and then discussed the advantages and disadvantages of RSA algorithm in IC card applications. RSA is easier to distribute than symmetric cryptography and is suitable for the open environment of IC card. Yet its secrecy needs strengthening. And RSA algorithm is more complex, if each IC card with different values, the amount of work is too large. Then they use formulas and theorems to explain how RSA algorithm is implemented in IC card.

RSA algorithm in IC card can be used for dynamic and static data verification and digital signature, finally they use theorem inference to verify the application of RSA algorithm in life data.

5. Conclusion

In general, the RSA encryption algorithm has a high degree of security, but this security stems from complex numerical calculations. Therefore, the decryption process will be relatively complex, and the computation speed is difficult to estimate. We also looked at ways to improve RSA encryption algorithms, such as using MPI or the Java language. In our real life, RSA encryption algorithm is also used in many places, like authentication system , smart medicine boxes and smart card.

References

[1] Yang Deyu, Lu Kuijun, Ya ngDe s ha n, e t a l. Design and implementation of an improved RSA encryption algorithm [J]. Computer Applications and Software, 2007, 24 (10): 188-189.

[2] Lu Qiyang. Application of MPI in RSA encryption algorithm [J]. Computer Knowledge and Technology, 2015, v.11 (28): 46-48.

[3] Zhu Shuji, Li Weiqin. An identity authentication system based on RSA encryption [J]. Small microcomputer system (8): 954-956.

[4] Li Fengling, Zheng 飞. Discussion on the application of RSA encryption algorithm on QR dimensional code [J]. Medium enterprise management andScience and Technology, 2014 (31): 207-208.

[5] Chen Fei, Li Shaoxuan. Application of improved RSA encryption algorithm in intelligent medicine box data storage [J]. Full technology and application, 2017 (4).

[6] Cao Junwei, Li Yi. Implementation and Discussion of RSA Public Key Cryptography Algorithm Based on Java [J]. Software Guide, 2011 (05): 89-91.

[7] Tu Hang, Liu Zhen, Zhang Huanguo, et al. Realization and application of RSA algorithm in smart card operating system% Realization and Application of RSA in Chip Operating System [J]. Wuhan University of ScienceReport (Science Edition), 2000, 046 (003): 313-315.

[8] Ca lde rba nk, Micha e l. The RS A Cryptos ys te m: His tory, Algorithm, Prime s (PDF). 2007-08-20.

[9] Elementary number theory p48.