Analysis and Research of Data Encryption Technology in Network Communication Security

Weiqiang Qi(✉), Peng Zhou, and Wei Ye

State Grid Zhejiang Electric Power Corporation Information and Telecommunication Branch, Hangzhou 310016, China

Abstract. With the rapid development of information technology, especially with the wide application of the Internet, the communication security in the network has become an important problem we have to face. In order to solve this problem, this paper takes the network report system of a mining enterprise as the research object, comprehensively expounds the design of network reporting system and data encryption in network communication from the aspects of demand investigation, demand analysis, system design and software system development, and develops and realizes it by using BS architecture + independent client. This paper first briefly introduces the background and significance of computer network communication security research, explains the importance of data encryption in network communication, and the development process and status quo at home and abroad.

Keywords: Network report system · File encryption · RSA algorithm · Design and development · System testing

1 Introduction

The development of information technology in today's world is changing with each passing day, especially after the emergence and popularization of the Internet. Nowadays, almost everyone is inseparable from the Internet, and they are always in contact with the Internet [1]. The number of Internet users in China is also increasing. Network anti-corruption, that is to expose the corruption behavior in life through network public opinion and network report, provides a new mode for government and enterprise anti-corruption. Under the background of the rapid development of Internet technology and anti-corruption, many governments and enterprise affairs groups give the greatest support and recognition to the report and the emerging network reporting system. In recent years, some staff of Beijing Donghua Yishi Technology Co., Ltd. have seen the great application prospect of this reporting system, and have designed and developed an online reporting system for some governments and enterprises. Here, I choose the construction project of the network reporting system of the grass-roots employees of a mining enterprise in Tengzhou that I participated in. In order to let the scientific, legal and democratic governance accept the comprehensive supervision of grass-roots employees, Tengzhou beixulou coal mine insists on keeping pace with the times and introduces the network security reporting system. The effective use of this system can play a great role in anti-corruption and daily production.

M. A. Jan and F. Khan (Eds.): BigIoT-EDU 2021, LNICST 392, pp. 503–511, 2021.
https://doi.org/10.1007/978-3-030-87903-7_62

2 Analysis of Encryption Technology

2.1 The Importance of Data Encryption

With the progress of science and technology and the rapid development of information technology, people have enhanced the awareness of the protection of information, information security has become increasingly important, now people are paying more and more attention to information security, and began to explore the relevant processing methods [2]. Information is a macro concept, which is composed of data. In other words, data appears as a carrier. Therefore, we must take certain measures to protect the data security, to avoid the data being stolen or destroyed or intentionally modified. The best way to solve the problem of data security is to prevent data leakage through file encryption.

2.2 Principle of Data Encryption

We call the original information which has not been transformed into plaintext (P), and the information after transformation is called ciphertext (C). This transformation from plaintext to ciphertext is called encryption (E), and is usually implemented by some encryption algorithm. The process of recovery transformation from ciphertext to plaintext is called decryption (d), which is usually implemented by some decryption algorithm. As shown in Fig. 1 below.

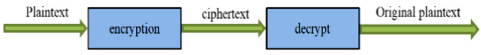

Fig. 1. Data encryption principle model

The sender encrypts the plaintext P into ciphertext and sends it to the receiver. After receiving ciphertext C, the receiver uses the corresponding key for decryption to restore ciphertext C to the original plaintext P [3]. In this way, even if the information in the transmission process is stolen by others, he can only get ciphertext C. without the decryption key, he can't understand it, which plays a role in protecting the information. When encrypting, the encryption key we use is the parameter K, where k is only one randomly selected from the key space, and we can also select any other value. If only one key is used, then this is symmetric encryption technology using symmetric key, and the shared key is K.

The purpose of adding activation function to the network is to add nonlinear mapping with nonlinear factors to enhance the nonlinear expression and fitting ability of network model. The main expressions of the activation function are 1, 2 and 3 of the activation function of CNN.

$$sigmoid : f(x) = \frac{1}{1 + e^{-x}} \tag{1}$$

$$\tanh : f(x) = \tanh(x) \tag{2}$$

$$\mathrm{Re}LU : f(x) = \max(x, 0) \tag{3}$$

3 Analysis of Classical Encryption Algorithm

3.1 Overview of Encryption Algorithm

The encryption algorithm obviously is to process the data to be transmitted into the data that can't be understood by outsiders, and then transmit it to the correct receiver, and then the receiver will restore the ciphertext processing and read the information with the agreed processing method in advance. In this way, even if the interceptor is intercepted on the way, the information cannot be read after intercepting because the interceptor has no corresponding decryption algorithm.

There are two major classes of encryption algorithms. One is the earlier one, which is not based on key. This premise is that the algorithm is confidential, just like the connection code. The disadvantage is obvious. If the algorithm is leaked or cracked, it will not be available. The other type is naturally based on key, which is commonly used by us now. Key is generated by the algorithm, the algorithm is public, but the key is confidential, so only need to change the key, no need to change the algorithm, so it is much more flexible. The guarantee of security falls on the key, and the length of key determines the security. Symmetric encryption and asymmetric encryption are two kinds of key based encryption algorithms. The previous chapters have already been described, so I will not repeat them here. The following introduces and analyzes several commonly used encryption algorithms, and selects the encryption algorithm adopted by the encryption and decryption client.

3.2 DES Algorithm

DES, also known as data encryption standard, is a very classic symmetric encryption algorithm. It was first developed by IBM company, and then developed as data encryption standard by the United States and ISO. DES is a group symmetric encryption and decryption algorithm. Before encrypting the plaintext, all plaintexts are divided into multiple groups, and the length of each group is set to 64 bits. Then the binary data encryption operation of each group is performed. After encryption, a group of 64 bit ciphertexts are generated. Finally, the ciphertexts of each group are spliced together to get the whole ciphertext. The length of the key used is 64 bits. It should be noted that 8 bits are used for parity check (see Fig. 2).

DES algorithm involves, of course, the three parameters that are usually involved in the algorithm: the original or processed data or information, the suitable key generated according to the algorithm, and the running stage mode [4].

The specific operation process of DES is as follows: when the working mode is switched to the encryption mode, the plaintext is encrypted with the preset key, and then the ciphertext is generated and the output is generated; when the working mode is switched to the decryption mode, it is processed with the preset key, and then the correct information is recovered and the output is generated. Before data transmission, both parties agreed in advance obtain the same key according to the corresponding method. Before data transmission, DES algorithm is used to encrypt the data, and then the encrypted information is transmitted to the place where it needs to be reached. After the data arrives at the correct place, the data receiver decrypts the data with the same

secret key [5]. Obviously, for outsiders who do not know the key, it is necessary to use the same secret key to decrypt the data, This is enough to ensure the security of data transmission (see Fig. 2).

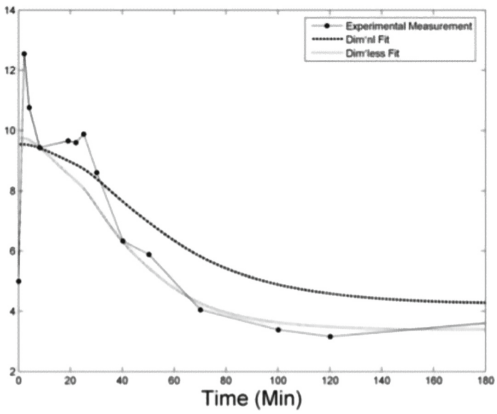

Fig. 2. Simulation with DES algorithm.

3.3 MD5 Algorithm

The main purpose of MD5 is to ensure the correct transmission of information [6, 7]. The specific implementation process is as follows: for example, I generated a text document, and then generated an MD5 value. I release this file for others to download and use. When the download person is not sure whether the file is safe or it is suspected to contain a virus, MD5 can be used to verify. If the value is the same, then it is safe. If it is not the same, it is modified and dangerous! There are many MD5 small programs on the network, mainly used to verify data integrity. Thus, MD5 is widely used, and its security and reliability are also relatively mature [8].

The principle of MD5 algorithm can be summarized as follows: MD5 does not require the length of input information, but the output must be fixed to 128 bits. The basic methods of its implementation include finding the remainder, taking the remainder and adjusting its length, and performing cyclic operation with linked variables [9].

Through the above analysis, we conclude that the main purpose of MD5 is not consistent with the project we are going to do. Because the most important thing we need to do is to ensure that the reported information is not stolen by others, not just to ensure that the reported information is not tampered with. In addition, MD5 is not enough to ensure the security of information. As early as 2004, a professor from Shandong University had decoded MD5, so we rejected the MD5 algorithm. Therefore, it is no longer necessary to elaborate, and only the next section describes the flow of the algorithm [10].

Although RSA is the first proposed public key algorithm, it is also a very comprehensive public key algorithm. It can not only be used to encrypt all kinds of information, but also has great use in signature and authentication. This algorithm is the most widely

used and trusted algorithm. Since the date of release, it has been attacked and cracked by scholars and hackers, but no one can crack it successfully [11]. Of course, it is undeniable that we can not use scientific means to prove that it can not be cracked, but countless facts have proved that it is reliable and its security is guaranteed. Therefore, RSA today is very important, can be said to be indispensable, has been adopted to a high degree (see Fig. 3).

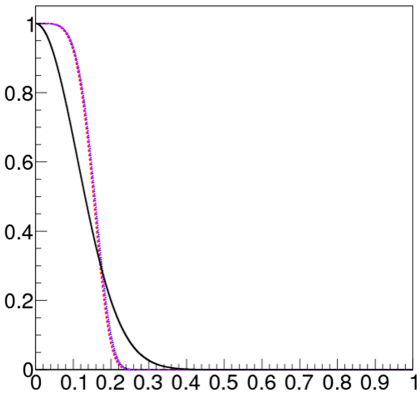

Fig. 3. Simulation with MD5 algorithm.

4 Design and Implementation of RSA File Encryption in the System

4.1 The Client Function of Encrypting and Decrypting Report Files

(1) The key can be generated and decrypted for the client only. 2) The client can load any public key or private key. Both the employee client and the administrator client have this function. (3) The client can load the txt file with the report content encrypted by the public key, and then the ciphertext can also be saved as the txt file. Only the employee client has the encryption function. (4) The client can load the private key to decrypt the ciphertext TXT file, and then save the plaintext as the txt file. Only the administrator client has the decryption function. (5) To emphasize one point, ordinary employees use the encryption client. Generally, the public key loaded by them is released by the administrator (who also owns the decryption client) and downloaded by ordinary employees. In this way, the key pair can be updated regularly to ensure more security! To sum up, the employee client can load the public key (download the public key from the server) to encrypt the file, And save the public key and the encrypted ciphertext. The administrator client can generate and save the key pair, upload the public key to the designated server, decrypt the ciphertext of the report file with the corresponding private key, and save the decrypted plaintext [12].

4.2 Technical Route Selection

Based on the actual situation of client development, this paper analyzes and compares several common technical means, and combined with their own familiarity, finally selects the best technical route, and tries to use easy to learn and easy to use Python language to write the client [13]. (1) Development based on Java platform the workload of client development based on Java is not large, because the Java class library provides complete RSA tool classes, including encryption, decryption, key pair generation and other methods. Therefore, it does not need to write too much code to complete, and one advantage is that it can cross platform. However, as we all know, Java must have its virtual machine, so the efficiency will be discounted, and because of its cross platform nature, it can't be as close to the operating system as other languages, so we don't choose it. (2) Net platform is a relatively new integrated development environment, which is convenient for rapid development and highly efficient. In addition, the. Net platform provides a very powerful class library. The first choice is C language. C # has many desktop applications on Windows platform. The client interface developed by C # is delicate and easy to use. Because of its many class libraries and controls, programming becomes relatively easy. Net provides encryption and decryption classes, RSA support class is RSA crypto service provider, so the development can be completed relatively quickly [14]. One of the disadvantages is that the system must be equipped with net framework. The other one is that it is less efficient than localized code. (3) Python based development language is simple and easy to use, with simple implementation logic and enough performance. As we all know, in design, the simpler the logic is, the higher the reliability is, and the less likely it is to make mistakes! Python is an interpretive language, which can be executed directly without compilation, which can improve the speed of development and testing, and facilitate subsequent modification and function improvement. Secondly, Python is very convenient for the large number storage operation in RSA algorithm compared with C++, because it is a dynamic type and can automatically adjust the storage type according to the needs. In addition, python can package programs directly without the limitation of additional support like Java virtual machine or net framework, so it has good cross platform performance [15].

Considering the software's executability, maintainability, reusability and development workload, the software adopts layered implementation, and the underlying RSA algorithm is encapsulated into a reusable RSA encryption and decryption library by python, which is called by the upper layer. WxPython, a GUI library, is used in the upper graphical interface. The library is based on wxWidgets cross platform GUI tool library developed by C++. It can run in Microsoft Windows system, almost all uni "X" and similar systems without changing the code. Of course, Mac OS can also be used. The advantages of this development are: the main functions are at the bottom and can be easily improved, extended and modified. As mentioned above, this client development is divided into three parts: using Python to write RSA algorithm, encapsulating it into a reusable RSA encryption and decryption library, and using wxPython, the Gu graphics library, to realize the graphical interface of the basic operation of the client [16].

4.3 Design and Implementation of Encryption Algorithm

The main function modules that need to be developed are: (1) generation of key pair (only administrator client has this function); (2) encryption and decryption of file by loading key (appearing separately in employee and administrator client); (3) opening and saving of text file and uploading and downloading operation (common); (4) encryption and decryption of file by loading key; (4) Design and production of graphical operation interface (common). This section focuses on the generation of key pair, the encryption and decryption operation of loading key pair file. From the analysis in Sect. 3, we can know that the basis of RSA is large number and its operation. Therefore, the design and implementation of encryption algorithm can be summed up in the following three aspects: the first is the search and test of large prime number, the second is the generation of public key and private key, and the last is the encryption and decryption of TXT report file. The search and test of large prime number is the most fundamental and the first. If there is no large prime number, there will be no RSA algorithm. Generally, we search and constantly test to find out and determine the appropriate large prime numbers P and Q in RSA algorithm. The generation of RSA key pair is actually the generation of public key for encryption and private key for decryption, and whether the key is reliable and secure. This fundamentally defines the security of this security system, We need methods to generate extremely secure and reliable trusted key pairs. Another important operation is encryption and decryption. The main operation involved is modular exponentiation, which fundamentally defines whether this algorithm is effective and fast. Obviously, we need an efficient algorithm, but at the same time, it is used for small TXT text encryption and decryption, so this requirement is not too high, and sufficiency is the most basic [17].

5 Software Implementation of Generating Large Prime Number

Here is an important point to declare. So far, it is very difficult for computers to generate a large prime number randomly. If we want to ensure that we can get a relatively accurate large prime number, we need and must get it by looking up the prime table. But this way is dangerous, because if this vital prime table is stolen, then the reliability and security of RSA algorithm in this way is questionable. Originally, we wanted to adopt this method. Later, considering the possible security problems, we gave up. Now we use random calculation to generate large prime numbers. In this way, the disadvantage is that it greatly increases the complexity of the algorithm, and the advantage is that it greatly improves the security of the system. This method can't guarantee 100% generating primes in a short time, just try to find the right P and Q by searching and testing.

Prime numbers are infinite, that is to say, the number of prime numbers is countless, which has been proved. Although a lot of efforts have been made, there is still no solution for factoring large integers! This proves that a method of producing prime numbers is not feasible, that is, by trying to factorize large integers. So far, the most effective way to find large prime is to judge whether a large integer can pass the test of some prime detection algorithm.

6 System Test

6.1 Test Purpose

The purpose of system testing: 1. System as a whole: all functions of the reporting system are correctly implemented in accordance with the requirements of customers, without defects affecting its normal operation, and the performance indicators have reached the standards set by the industry and customers. 2. Function: ensure that the reporting system can operate correctly and realize various functions correctly when it is used on a centralized scale in the company. 3. Performance: ensure that the reporting system can meet the large amount of data inquiry, multi-user concurrent operation, the number of failures or errors and the maximum or average response time of the system are within the normal range. 4. Security: the report must have a complete user rights management function, all files storing passwords must be encrypted, the system must transmit key data in the network environment, and the transmitted data must be encrypted twice.

6.2 Test Scope

The whole system test includes the following process: 1 module test: each functional module should be tested several times to see whether each module is normal. If not, the statistics of error probability and error reason should be done for subsequent modification. 2. Integration test: after the establishment of the reporting system, test whether the business links between different modules are normal. 3. Confirmation test: check whether the reporting system can meet all the functional and non functional requirements mentioned in the customer requirements. 4. System test: check whether the reporting system and the corresponding client can operate normally in the real environment and have good compatibility. 5. Acceptance test: after the system is tested by us, it needs to be tested by the customer to let the customer judge whether it meets the customer's needs.

This test includes functional test and non functional test, the details are as follows: (1) functional test (2) performance test (3) user interface (UI) test (4) interface test (5) security and access control test (6) failure transition and recovery test (7) fault tolerance and exception test.

7 Conclusion

In a word, in the new era, network communication data encryption technology has obtained rapid development, and data encryption technology has been widely used in various industries and fields. The relevant technical personnel must strengthen the research, further optimize and improve the data encryption technology, create a good network communication environment for users, and promote the sustainable and healthy development of computer technology.

References

1. Xiaosong, Z.: Application of data encryption technology in computer network security. J. Jiamusi Vocat. Coll. **07**, 254–255 (2019)

2. Xiangna, C.: Exploring the application of data encryption technology in computer network communication security. Netw. Secur. Technol. Appl. **6**, 23–24 (2019)
3. Xue, H.: Research on data communication network maintenance and network security. Electron. Components Inf. Technol. **2**(08), 6–8+17 (2018)
4. Xu, Z.: Analysis of data encryption technology in network communication security. Comput. Prod. Circ. **2019**(11), 28+30 (2019)
5. Zou, H., Xu, P.: Introduction to Cryptography. People's Posts and Telecommunications Press, Beijing (2004)
6. Lecai, C.: Applied cryptography. China Electric Power Press, Beijing (2005)
7. Wei, R.: Modern cryptography. Beijing University of Posts and Telecommunications Press, Beijing (2011)
8. Chen, Z.: Implementation of RSA public key cryptography software package. Master's thesis of Guangzhou University (2002)
9. Xie, X., Wei, B.: Analysis of network information encryption technology. Science and Technology Plaza (2007)
10. Jian, Z.: Cryptography Principle and Application Technology. Tsinghua University Press, Beijing (2011)
11. Yuefei, Z., Yajuan, Z.: Public Key Cryptography Design Principles and Provable Security. Higher Education Press, Beijing (2010)
12. Report on the Development of Cryptography in China, Group of Chinese Cryptography Society. Electronic Industry Press, Beijing (2011)
13. Xueli, W., Dingyi, P.: Theory and Implementation of Elliptic and Hyperelliptic Curve Public Key Cryptography. Science Press, Beijing (2006)
14. Xiaoyong, G., Yang, F.: Network Security Operation and Maintenance. Higher Education Press, Beijing (2011)
15. Xiaohua, Z.: Computer Network Security Technology and Solutions. Zhejiang University Press, Zhejiang (2008)
16. Ma, G., Bai, Y.: Analysis of RSA public key system technology and design of related algorithms. Comput. Sci. **33**(8) (2006)
17. Shi, X., Dong, P.: Design of a new encryption core based on RSA algorithm. Microcomput. Inf. **12**, 3 (2005)