Computing, Performance and Communication Systems (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/cpcs.2022.060207
ISSN 2371-8889 Vol. 6 Num. 2

Research on Public Key Cryptography System Based on Network Information Security

Houding Zhang

University of Wollongong, Wollongong, Australia
hz138@uowmail.edu.au

Keywords: Public key, Digital encryption, Information security

Abstract: Affected by viruses, hackers and other factors, computer network security incidents have shown a high incidence in recent years. The biggest advantage of the public key system is that it doesn't need to keep secret the key communication, only the public key needs to be transmitted, thus saving a costly key transmission channel. The network needs to strengthen the construction of public key cryptosystem, protect data information by various digital encryption methods, ensure the security of information, and meet the actual use needs of users. This paper expounds the basic principle and advantages of public key encryption algorithm for network information encryption, and explains how to apply public key encryption technology to identity authentication and digital signature technology.

1. Introduction

With the popularization and growth of IT and network technology, global IT has been widely used in all walks of life. After entering the 21st century, the world has entered the network era, and modern society has increasingly relied on information systems built by computer networks, and the security of computer networks has been paid more and more attention by people [1]. This is not only because the possibility of data information in the computer network being stolen, copied, leaked or modified in the process of storage and transmission is constantly expanding, but also the factors that threaten the security of the computer network may come from many aspects, including some imperfections that may exist in the computer network itself [2]. In the Internet age, the computer network provides a convenient channel for the dissemination and reception of information, greatly improving the speed of information dissemination, and significantly improving people's work efficiency [3]. However, in view of the operating characteristics of computer network, it is easily affected by various unsafe factors, and there are problems such as data loss or leakage, which bring some hidden dangers to people's own information security [4]. The biggest advantage of the public key system is that it doesn't need to keep secret the key communication, only the public key needs to be transmitted, thus saving a costly key delivery channel.

To construct the public key and private key in RSA encryption and decryption algorithm, we must first construct two large prime numbers. The security of RSA encryption and decryption algorithm is closely related to the large prime number used. Therefore, studying the generation of large prime numbers in RSA public key system and constructing strong prime numbers that meet the requirements of RSA security system is the foundation of practical application of RSA algorithm [5]. Under the background of networking, interconnection and sharing has become a way of life and work. The growth of computer continues to speed up, and the dependence of residents' life and work on the network is gradually increasing. Frequent computer network security incidents have aroused great concern from all walks of life. Based on this, relevant technical personnel should improve their awareness of security and use corresponding data encryption scientifically to ensure the security of data transmission and storage, and provide reliable guarantee for the safe operation of computer networks [6]. Data encryption is a widely used network security management and prevention technology. This technology mainly protects the process of information analysis and dissemination through the application of encryption technology [7]. Big data can not only retrieve effective information, but also has a unique way of thinking change, which can reflect its existence value. The characteristics of data encryption can systematically analyze data information in all directions. This paper expounds the basic principle and advantages of public key encryption algorithm for network information encryption, analyzes RSA algorithm, and explains how to apply public key encryption technology to identity authentication and digital signature technology.

2. Application Value of Encryption Technology in Computer Network Security

2.1 Evaluate Safety Level

With the advent of the era of big data, technologies such as big data storage and big data analysis have been extended, and the work efficiency has been improved based on big data analysis methods. Big data technology combines the advantages of IT and Internet science and technology, and strictly controls it through digital way to ensure the accuracy of data information [8]. Data encryption is an important technical means under the background of network security, which can greatly guarantee the network security of computers. Therefore, this technology is also used as an important index to evaluate the defense force of network systems. All sectors of society can't do without the support of IT, and its working principle is to scientifically control data resources with the help of programming system.

The security of any encryption method depends on the length of the key and the amount of computation required to break the ciphertext. In this respect, the public key cryptosystem is not superior to the traditional encryption system. Because the current public key encryption algorithm costs a lot, it is impossible to give up the traditional encryption method in the foreseeable future. The public key cryptosystem is shown in Figure 1.

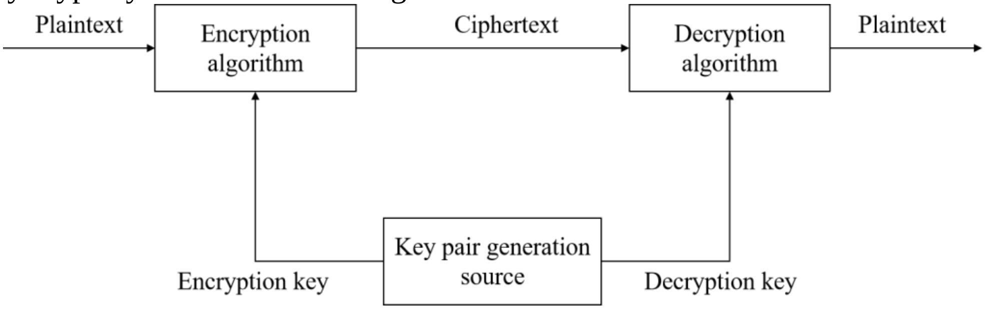

Figure 1: Public Key Cryptosystem

According to the analysis of the current operation status of China's computer information industry, big data IT can not only achieve automation, but also provide convenience for the realization of data information intelligence. The stronger the application ability of encryption technology in the network security system, the stronger the defense and the higher the stability of this network architecture. Through the encryption technology used in the network system, we can have a preliminary understanding of the whole network security. Under the traditional mode, computer network secrecy is difficult to adapt to the development speed of computer network technology. The application of scientific data encryption can effectively improve the efficiency of computer network security management, and regulate and adjust the computer network management system, so as to ensure the safety of computer network operation.

2.2 Improve Defence Ability

Modern information management technology can provide a convenient foundation for industrial transformation and upgrading. At present, IT is widely used in various fields of society. On the basis of the rapid growth of network technology and continuous optimization of data information, the traditional form of data search is difficult to meet the current demand [9]. The growth of data encryption is not only a growth of algorithms, but also a technical assembly based on the whole network system. This means that the application of data encryption can not only be used as a starting point to improve data security, but also as a starting point to improve the stability of the whole transmission process. The principle of network intrusion detection is shown in Figure 2.

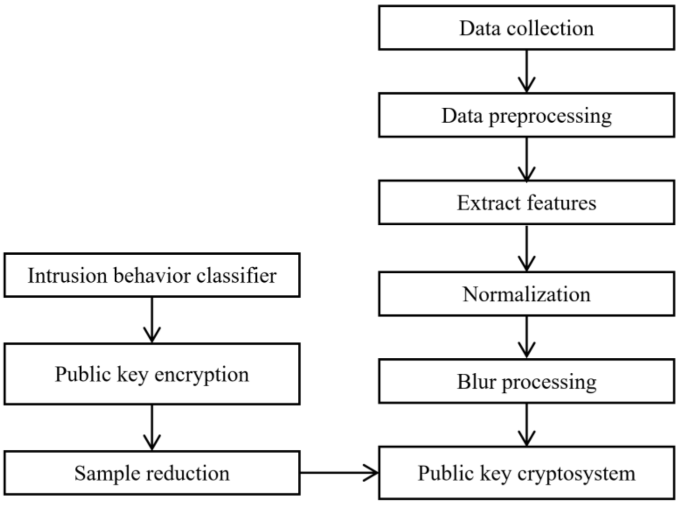

Figure 2: The Principle of Network Intrusion Detection

In order to obtain constructive information resources, it is necessary to go through complicated links and steps, and it is also necessary to conduct in-depth data mining to ensure the accuracy of data information [10]. Under the condition of network security technology, the application of data encryption is often not a single encryption, but a combination of various encryption technologies to enhance the defense of data security. Data encryption can transform the industrial structure, innovate and optimize the management mode, and make it occupy a place in the highly competitive market environment, thus providing a fundamental guarantee for enterprises to achieve sustainable development.

3. Public Key Cryptosystem and Data Encryption

3.1 Node Encryption

With the continuous growth of encryption technology, there are more and more types of encryption technology applied in network security operation and maintenance, which has an important supporting significance for network security. The essential purpose of encryption technology development is to provide a certain guarantee for the data operated in the network, so as to avoid the loss or malicious rewriting of information in the link of uploading or downloading. At present, in the use of data encryption, node encryption technology is one of the common encryption technologies. From the feedback of technology application, this technology can better improve the security performance of data, which is conducive to the improvement of the security performance of the entire network. RSA public key cryptosystem involves a lot of numerical computation in the change of encryption or decryption, and the operation time of encryption and decryption is relatively long. Therefore, the actual use of RSA cryptosystem must use VLSI (Very Large Scale Integration) hardware products.

3.2 Link Encryption

Compared with node encryption technology, link encryption technology is superior in application effect [11]. It mainly implements the encryption of node links, so that the data encryption operation in the network can be completed. In the conventional key cryptosystem, both sides of encryption and decryption use the same key. Public key algorithm is the best cryptographic algorithm at present. It can be used not only for encryption but also for digital signature, that is, the receiver of information can verify the identity of the sender. The sender can't deny the signed information after sending it, and issues the public key certificate, issuing certificate, managing certificate, etc. for the user's public key. This makes it possible to protect data more securely.

3.3 End to End Encryption

End-to-end data encryption does not need to use all the encryption in the data transmission process to realize the encryption and decryption of intermediate nodes, so there is no high requirement for the security encryption protection level of nodes. End-to-end encryption technology is gradually applied in the current network security operation, which to a great extent represents a direction of data encryption in the current network security technology. In the process of application, the advantages of end-to-end encryption technology have also begun to emerge. Its design cost is relatively low, and the independent encryption method is adopted in its application process. In the case of errors in some transmission lines, it will not affect the data packets of other lines, so it has very high reliability and is convenient for daily maintenance. Compared with node encryption technology and link encryption technology, end-to-end encryption technology can encrypt the whole data transmission process, that is, realize the uniform encryption from the beginning to the end of data.

4. Conclusions

The growth of technology is a double-edged sword. While opening the era of sharing and data, it also makes network users face more problems and greater challenges. With the research and growth of new technologies, such as the fast algorithm for the generation and detection of prime numbers, the implementation technology of modular exponentiation of large numbers, the parallel algorithm, the storage technology of large numbers, etc., the practicability and application scope of public key cryptography are constantly expanding, and its security advantages will be fully exerted. If the password in a cryptosystem can't be deciphered by available computing resources, then this cryptosystem can be regarded as computationally secure. The construction of public key cryptosystem can create a safe and reliable environment for people to apply computers, and effectively avoid the destruction of viruses and illegal programs. Network security problems occur from time to time. To effectively protect network information and data, it is necessary to strengthen the update and maintenance of computer software and hardware, strengthen the standardization and security awareness of network users, take timely and effective measures and rationally use various protective measures such as firewalls in view of the current network security problems such as computer software and hardware vulnerabilities and virus attacks.

References

[1] Wang Qin. Discussion on computer network information security and encryption technology [J]. Science and Technology Innovation and Application, 2021, 11(33):4.

[2] Zhang Dapeng. Design of computer network information security optimization encryption algorithm [J]. Digital Communication World, 2018, 160(04):128+202.

[3] Liu L, Chen W, Li T, et al. Pseudo-Random Encryption for Security Data Transmission in Wireless Sensor Networks[J]. Sensors, 2019, 19(11):2452.

[4] Jiang Mingfu. Design of network information security encryption system based on chaotic sequence [J]. Modern Electronic Technology, 2018, 41(23):84-88.

[5] Xu Lijuan. Research on Data Encryption Technology in Computer Network Information Security [J]. Modern Communication, 2017(17):1.

[6] Shen Haitao. Application of data encryption in network information security [J]. Digital Technology and Application, 2019, 37(2):2.

[7] Li L. Integration of information security and network data mining technology in the era of big data[J]. Acta Technica CSAV (Ceskoslovensk Akademie Ved), 2017, 62(1):157-165.

[8] Wang S, Zhu L. A markov game model of network security in information system based on copula theory[J]. Boletin Tecnico/Technical Bulletin, 2017, 55(12):227-232.

[9] Shin J, You I, Seo J T. Investment Priority Analysis of ICS Information Security Resources in Smart Mobile IoT Network Environment Using the Analytic Hierarchy Process[J]. Mobile Information Systems, 2020, 2020(3):1-11 .

[10] Jiang Xiaowei. Research on Encryption Algorithm and Application of Network Information Security Center [J]. Information Weekly, 2018(17):1.

[11] Liu Xiao. Network Information Security Data Encryption Technology in Computer Foundation [J]. Electronic Technology and Software Engineering, 2019(9):1.