Application of Data Encryption Technology in Computer Network Communication Security in Information Age

Jinyan Zhang

School of Communication Engineering, Beijing Jiaotong University, Beijing 100044, China

19721077@bjtu.edu.cn

Keywords: Computers; Communication security; Data encryption; Application

Abstract: The application of data encryption technology in computer network communication security is to ensure the safe transmission and storage of information. The development of the Internet has brought great convenience to people's life and work, but it has also caused certain security problems. Encryption of data in computer network communication security is an effective way to protect information and data, and is also one of the most effective methods to ensure the safe transmission of network. Therefore, it becomes more critical to further strengthen the prevention and treatment of related computer viruses under the network environment, of which data encryption technology is the most important measure. This paper makes a simple analysis of the application of data encryption technology in computer network communication security technology in order to provide reference for relevant personnel.

1. Introduction

Based on the field of modern society, network information technology has now become an important means of information transmission, which can promote people to obtain all kinds of information more efficiently and conveniently [1]. In the information age, information disclosure is a great loss. Virus infection, system vulnerabilities, hacker's invasion and so on may all lead to information disclosure. In order to protect the security of network data, it is necessary to pay attention to its security protection measures. In recent years, the problem of network security has been threatening us, seriously affecting our life and work. Privacy leaks and important data loss occur frequently. If data encryption technology is not applied properly, it will cause unnecessary troubles and losses [2]. Therefore, strengthening the research of data encryption technology can improve the level of network security. The better security and stability of data encryption technology enable people to use network communication technology more confidently. The application of data encryption technology in computer network communication security will be discussed in detail below.

2. Connotation of Network Communication and Data Encryption Technology

2.1 Network communication

Network communication usually refers to the network communication protocol, which mainly specifies the transmission code, transmission control steps, information transmission rate, error control, etc. Through the network protocol, computers can connect independent computers and integrate the functions of software, hardware and data sharing, thus timely processing and comprehensively and effectively maintaining data resources [3]. Most network communications refer to network protocols, which connect information communication and conversation. Network protocols control specified standards such as code transmission, information transmission speed and transmission steps.

  DOI: 10.25236/iwmecs.2020.002

2.2 Data encryption technology

There is a complete encryption system in computer network communication, which generally includes plaintext form, ciphertext form, decryption device and corresponding key algorithm, etc. By effectively organizing and utilizing these resources, it can effectively resist data theft and network attack of network information system. It usually means that a certain information is converted into a completely meaningless ciphertext after being converted by a key and a certain function rule, and the receiver can restore it into plaintext by relying on this key or rule. The algorithm used in the conversion of plaintext and ciphertext is not random, it is called key, and the data can be read normally only after using the corresponding correct key [4].

Computer network communication security means that there is a certain degree of confidentiality in the process of information transmission. In computer network communication security, the application principle model of basic data encryption technology is shown in Figure 1.

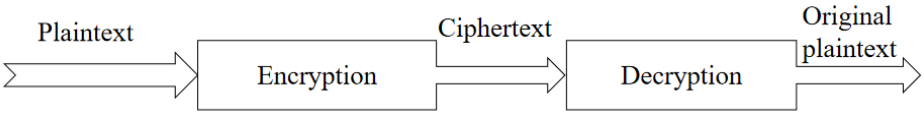

Figure 1. Application principle model of data encryption technology

When the information is completely transmitted to the user, the user decrypts it with the secret key to obtain the plaintext content. Because there is no secret key and the ciphertext cannot be decoded correctly, what you will see is a string of garbled codes, so that important data can be secured in the process of communication transmission. When the receiver receives the ciphertext, it can use the secret key to decrypt and obtain the plaintext.

3. Method of Data Encryption Technology

3.1 Symmetric encryption technology

Symmetric encryption technology is often used in computer network communication. This technology is very simple and effective in the process of operation, because it uses the same key for data encryption and data decryption. There is a security module in the node. This security module uses the device of password encryption to enable the node to encrypt in an unknown form, thus realizing the decryption and encryption of information. In addition, considering the convenience of encryption and decryption, this encryption method has been widely used, such as DES symmetric encryption method, which is widely used.

The detection scheme based on CDC algorithm improves the boundary offset problem of the fixed-length block detection scheme. According to the high efficiency of Rabin fingerprint calculation technology and the randomness of fingerprint function, it divides the file into blocks of different lengths [5]. Rabin fingerprint value is defined as follows [6]:

For any binary string $D=(c_1,c_2,\cdots,c_m)$, its corresponding polynomial is shown in Equation 1:

$$D(z)=c_1z^{n-1}+c_2z^{n-2}+\cdots+c_{n-1}z+c_n \tag{1}$$

$D(z)$ is a polynomial in c_2 domain, and Rabin fingerprint value $F(D)$ of binary string d is defined as shown in formula 2.

$$F(D)=D(z)\bmod Q(z) \tag{2}$$

Where $Q(z)$ is a reduced polynomial in c_2 domain, and its form is shown in formula 3:

$$Q(z)=x_1z^{i}+x_2z^{i-1}+\cdots x_{i-1}z_i \tag{3}$$

If the degree of $Q(z)$ is p, the length of $F(D)$ is p bits. At the same time, the detection technology based on CDC algorithm is divided into blocks according to file contents, and the size of data blocks is variable.

AES advanced encryption standard is the next generation encryption algorithm standard, with fast speed and high security level. Generally speaking, symmetric encryption is efficient, convenient and fast. The impact of node damage on information transportation is not great, even if one party is attacked maliciously, it will not affect the transmission of the following information. It can ensure the safety of computer network communication, and also can effectively improve the use efficiency of the method. Since the data is encrypted by different secret keys after decryption and then transmitted, the data is not displayed in clear text, so such secret keys are more reliable.

3.2 Asymmetric encryption technology

It is different from symmetric data encryption method. The main difference is that the key used for decryption and encryption is not the same. Therefore, there are two keys involved in this method, which are respectively called public key and private key. In general, asymmetric encryption has two sets of keys, namely "public key" and "private key". In the encryption process, the two sets of keys are used in pairs. Because the larger the key, the stronger the encryption, but the slower the encryption and decryption process. If only 2 bit are used to make this key, hackers can try to decrypt it with 0, 1 and 2 first, but if your key is 1 MB or more.

RSA algorithm is an asymmetric and very secure algorithm. As we know from the above, the biggest characteristic of this algorithm is that encryption and decryption adopt completely different keys. Under the common hardware environment, the calculation speed is faster, and all identical files in the data set can be detected at the same time, thus saving a large amount of storage space. However, this method also has two disadvantages: for large data sets, the comparison range is large and it takes a lot of time; In addition, the same data inside different files cannot be detected using this technology. At present MD5 and SHAl are widely used hash algorithms [7]. The performance comparison is shown in Table 1 [8].

Table 1. Comparison of SHA with MD4 and MD5

Serial number	MD4	MD5	SHA
Hash value	127bit	123bit	155bit
Packet handler	531bit	531bit	531bit
Basic word length	33bit	33bit	33bit
Number of steps	45(3*15)	60(4*25)	82(4*20)
Number of constants	3	62	5

RSA is a kind of asymmetric key, and it is extremely typical. Here, let's talk about its working principle: firstly, a key pair containing public key and private key should be generated. The public key, as its name implies, is public and is available to everyone. It is used for encryption and then transmits the encrypted data to the publisher of the public key. RSA key length cannot be too short, otherwise it will affect its reliability, generally we set it to 512 or 1024 bits. As shown in fig. 2 below.

In the process of data information transmission, there will be no decryption operation, thus ensuring that even if the node data is leaked, it will not affect the data security. Data is not decrypted before being transmitted to the receiver, and the whole transmission process is completely protected by encryption. This encryption method can effectively avoid the hidden defects of node encryption. If the computer network information system is invaded or attacked, the confidential system can effectively resist it, thus ensuring the security and reliability of computer network communication.

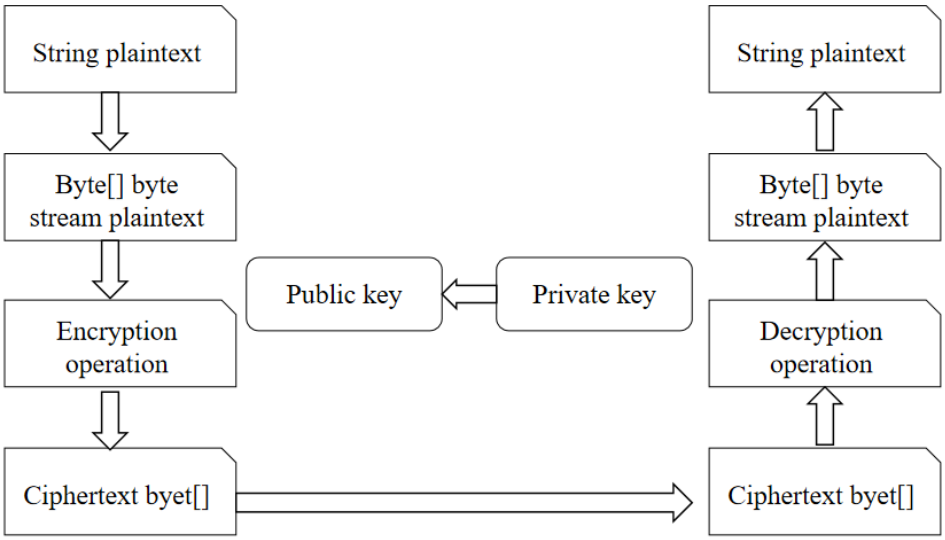

Figure 2. Illustration of the basic operation process of RSA.

4. Application of Data Encryption Technology in Computer Network Communication Security

4.1 Application in LAN

Many enterprises in modern enterprises set up corresponding local area networks in their management for data or meetings, etc. It is of great significance for the future development and normal operation of enterprises to do a good job in encrypting local area networks [9]. The encrypted data technology can be applied to the local area network, such as the information can be automatically stored in the local area network when it is sent, or the encrypted file can be automatically unlocked when it reaches the designated location. The information to be transmitted must be encrypted before it is transmitted, and then the data needs to be decrypted every time it passes through a node on the link during transmission, and then encrypted before it is transmitted to another link. Such as network transmission encryption, data file encryption, data storage security, login security, log management and system management security. If there is no effective protective measures, it will certainly bring very serious risks to the company and employees. The data encryption technology mainly encrypts the data information through routers and senders in LAN. Because the data packets are encrypted independently, even if there is a problem with one data packet, the transmission of other data packets will not be affected.

4.2 Application in computer software

The link encryption technology can effectively ensure the security of data transmission in the communication link network. It encrypts information before data transmission, then decrypts it between network nodes, and then encrypts it. In the process of decryption and encryption, it uses different keys to protect data security. When computer software is invaded by hackers from outside, the defense systems of some internal systems can timely prevent the intrusion and destruction of viruses. If the antivirus software is infected with a virus during data encryption, whether the program or data has a signature cannot be checked, so when encrypting the program, it is necessary to check whether the files that need to be encrypted or decrypted are virus-free. Because each node is encrypted and decrypted, the data security is effectively guaranteed. Once the user inputs the wrong password when operating the computer software system, the normal operation of the software system can be organized, thus realizing the safety guarantee of the user information and avoiding the information leakage problem. During the whole data transmission process, each node and link will be re-encrypted and decrypted, so the security is very reliable.

4.3 Application in electronic commerce

Because the information is fully and effectively protected in the whole transmission process, even if the transmission node is damaged, the problem of information leakage will not occur. The original intention of Internet design is only to provide users with a flexible and fast communication platform. To ensure the sustained, rapid and healthy development of electronic commerce, electronic transactions involved in electronic commerce need to be conducted through the Internet and do not have the security of commercial transactions. In order to really strengthen the protection of information and the authentication of users in e-commerce, it is necessary to establish effective safeguard measures for personal information to enhance the intensity of economic protection. In the end-to-end encryption process, the data receiving address is usually not allowed to encrypt, because in the data transmission process, the node that must pass through depends on the receiving address to determine how to transfer the data. It adopts asymmetric data encryption method. The key of the starting node is different from that of the following node. When conducting e-commerce activities, attention should be paid to the protection of users' personal information and identity authentication information, so as to ensure the security of the transaction process. Because this method does not require continuous decryption during transmission, its security is relatively high. However, end-to-end encryption also has defects, which cannot hide the starting point and receiving point.

5. Summary

Computer communication network security needs our full attention. It exists objectively. We should further strengthen the protection of communication security. For the current country, computer network security is receiving more and more attention. Data encryption technology is an important technology to ensure the strictness and security of data transmission. Although the current data encryption technology still has some deficiencies in some aspects, it can ensure the communication security to the greatest extent after some optimization in practical application. We will do a better job of preventing computer network communication to create a cleaner and harmless network environment. Data encryption technology can be truly completed only by relying on professional scientific operations and the confidentiality of users.

References

[1] Tang Juan. Analysis on the application of data encryption technology in computer network communication security [J]. Information Communication, Vol.160 (2016) No. 04, p. 192-193.

[2] Zhao Mengyu. Analysis of the application of data encryption technology in computer network communication security [J]. Computer Fans, Vol. 000 (2017) No. 007, p. 53.

[3] Dong Jialun. Application Research of Data Encryption Technology in Computer Network Communication Security [J]. Computer Fans, Vol. 000 (2017) No. 009, p. 14.

[4] Zhao Jielin, Lei Yong. Application of data encryption technology in computer network communication security [J]. Electronic Technology and Software Engineering, Vol. 124 (2018) No. 02, p. 236.

[5] Liu Wei. Application of data encryption technology in computer network communication security [J]. Information Recording Materials,Vol. 019 (2018) No. 002, p. 51-52.

[6] Bai Hongxuan. Application of data encryption technology in computer network communication security [J]. Digital Design (Part 1), Vol. 000 (2019) No. 008, p. 25-26.

[7] Li Hongyan. Analysis of the application of data encryption technology in computer network communication security [J]. Digital Communication World, Vol. 000 (2019) No. 006, p. 184-185.

[8] Guo Zhongying, Sun Changchun, Cui Jun, et al. Application of data encryption technology in computer network communication security [J]. Electronic World, Vol. 000 (2017) No. 019, p. 172-173.

[9] Wang Yupeng. Application of data encryption technology in computer network communication security [J]. Shandong Industrial Technology, Vol. 000 (2017) No. 007, p. 137.