# Analysis of Computer Network Encryption Technology

**Mulan Hu**

Jiangxi University of Engineering, Jiangxi, Xinyu, 338000, China

**Keywords:** Analysis, Computer Network, Encryption Technology

**Abstract:** With the continuous advancement of data encryption technology in computer network security, the standards for network security have gradually improved. Experts pointed out that the creation of computer network security system has greatly helped the effective processing of data, which brings about the wide application of data encryption technology. This paper first analyzes the influencing factors of computer network data security, and then discusses the composition, algorithm, types and characteristics of data encryption technology and its application in computer network security, and proves that data encryption technology is an indispensable part of network security.

## 1. Introduction

With the popularity of computer network technology and the increasing participation of people in online life, the operational risks of computer network systems are increasing, and the confidentiality and integrity of various network information data are gradually threatened. Under the circumstance, computer network security has become an important task of Internet maintenance, and data encryption technology with good security and maintenance has emerged as the times require and has been fully developed. At present, data encryption technology has been widely used in a variety of computer network-led industries. Computer network researchers in many countries around the world are also actively involved in the research and improvement of data encryption technology [1]. In practical applications, there are many types of data encryption technologies, which have good practicability and high flexibility. Systematic research on the application of data security technology in computer network security can provide reference value for maintaining the safe operation of computer network and the integrity and confidentiality of network data information.

## 2. Overview of Computer Network Security and Data Encryption Technology

Computer network security mainly means that the hardware, software and system data in the network system are properly protected. The system information data is not changed, leaked and destroyed due to various accidental factors and malicious intrusion. The network system can run safely and smoothly for a long time. The network server continuously provides services without interruption, and is capable of resisting various network infringements, ensuring information integrity, confidentiality, and non-destruction of the computer network system.

Data encryption technology is the basic technology to ensure the security of network system information data. It is generally based on cryptography, and the explicit information in data transmission is encrypted by function encryption or key encryption, so that the information data is only Can be cracked and used by a specific group of people, the specific population receiving the information data through the corresponding decryption method to achieve decryption of information data ciphertext, to ensure that other people or other systems can not peek, steal and destroy this part of the information data, only a specific group can be related The use of information data is queried to achieve the security of computer network information data.

DOI: 10.25236/eeems.2018.030

## 3. Analysis of the Principle of Data Encryption Technology

Data encryption technology mainly involves plaintext, ciphertext, algorithms and secret keys. When the original untransformed processing information is called plaintext, it is relatively easy to understand, and the processed information content processed by plaintext is called ciphertext, which is difficult to understand. The conversion process from plaintext to ciphertext is data encryption, which is generally implemented by a specific encryption algorithm. In the process of recovery from ciphertext to plaintext, it is called data decryption. In general, it is implemented by a decryption algorithm corresponding to the encrypted data algorithm.

The computer network information data encryption processing link and the data decryption processing link also involve the sender and the receiver. After the plaintext processing and transformation, a ciphertext is formed, and the ciphertext is sent, and the sender is called the sender at this time, and the receiver receives The recipient of the ciphertext is called the recipient. The sender encrypts the plaintext, forms a ciphertext after the encryption operation, and then transmits the location of the receiver on the basis of the ciphertext. After receiving the ciphertext, the recipient uses the secret key to decrypt the ciphertext and decrypts the ciphertext to form the original plaintext. In the case of information stealing in the transmission mode of this mode, the computer attacker can only obtain the original ciphertext, and cannot resolve the file without the secret key. In this way, the computer network information can be protected.

The algorithm and the secret key are two important elements in the computer encryption process. The encryption algorithm mainly transforms the original easy-to-understand plaintext, and performs arithmetic processing and transform processing in the form of a secret key, followed by complex ciphertext generation. The data encryption technology mainly covers two core forms, namely symmetric encryption technology and asymmetric encryption technology. The algorithms are also diverse, and the strict and fixed unified industry constraint standards are to be determined. Both the secret key and the algorithm are very important in the process of computer network information security data encryption, because the secret key is actually within the scope of the algorithm, and the secret key is a specific algorithm.

Under normal circumstances, the library can be directly encapsulated in the program, and there is no redundant operation flow in the calling link, which can be conveniently used for data encryption operations. Obtaining the data information encryption key parameters by random extraction, of course, it can also be considered to filter any type of arbitrary value, assuming that the number of keys is only 1. At this time, the same type of secret key is used in the data encryption process and the data decryption process, which is called For the shared key, this encryption method is symmetric encryption technology. Data encryption and decryption process key types can be called asymmetric. The advantages and disadvantages of symmetric encryption technology are very obvious. The encryption and decryption speed is faster, but it is easy to crack. The asymmetric encryption technology has the characteristics of high security. Therefore, different algorithm types should be selected correspondingly.

## 4. Data Encryption Technology Key Distribution Management

Computer network information must ensure communication security, and data encryption technology requires certain confidentiality, identification, integrity and certainty. The primary responsibility is confidentiality, because confidentiality is the most fundamental, and plaintext protection bears the brunt, aiming to prevent information theft. The identification mainly refers to the legality review of the sender's document information in the ciphertext acceptance state, excluding the possibility of outsiders. This mode is identity recognition; integrity characteristics are easy to understand, and after the ciphertext receiving link is guaranteed, it is necessary to ensure information security in depth. Such information must be complete and not subject to negative processing and illegal damage; It means that the recipient accepts the message to determine the legitimacy of the sender and to prevent the phenomenon of repudiation. The key distribution management problem of data encryption technology design is an important part of the whole process.

The symmetric key is a key that needs to be involved in the details of the operation of the entire symmetric encryption process. Regardless of the number of people, regardless of the decryption operation or the encryption operation, the confidentiality of the secret key cannot be changed, and it cannot be made public. In the entire encryption process, the sender encrypts the original data by secret key, and the receiver can receive the encrypted file normally. The required key in the decryption process is equivalent to the former. Only in this way can the data decryption work be completed, and the decrypted and restored plaintext is Data information transmitted. The above encryption technology is simple and convenient to implement, and its operation speed is relatively fast. However, from the above data encryption and decryption process, it can be found that the participants in the entire link need to have a secret key, and the same secret key and the same type of secret key can be used. While the number of participants is increasing, the key supply should be followed, but such operations are more difficult and the security is reduced compared to the past.

The asymmetric type of key is designed to solve the above problems. Such a secret key is essentially a public key, and the public key is easy to obtain for foreigners. In computer network communication security, the data encryption technology uses a private key. Such keys cannot be disclosed to the outside world and are produced in private form. The adverse effects of symmetric key on computer network information security are mainly divided into two aspects: the management and distribution method of the secret key itself and the security of secret key transmission. The sender and receiver must obtain a copy of the secret key in a secure manner and must secure the key. If someone finds the key and knows the algorithm, all communications using that key are readable [2].

The asymmetric type key avoids the above two problems. Such a secret key is essentially a public key, and the public key is easy to obtain for foreigners, while the data encryption technology used in computer network communication security uses a private secret. Key, such a secret key cannot be disclosed to the outside world and is produced in a private form. The public key is published by its owner, and the private key must be kept secret. The information is transmitted by the sender using the recipient's public key to encrypt the data. Once encrypted, only the recipient can decrypt it with his private key.

Since the network transmission process only transmits the public key, even if the public key is obtained by others in the middle, there is no need to worry about information leakage. At the same time, the participants in the whole process need to have the secret key and the same key to threaten the security, fully comply with the confidentiality, identification, integrity and certainty characteristics of the data encryption technology requirements. On the other hand, the private key is used to encrypt the data, the encrypted information and the public key are transmitted, and the receiver decrypts it, and the sender can be digitally verified.

## 5. The Main Types of Data Encryption Technology

The main feature of symmetric data encryption technology is the use of the same key by encryption and decryption. In symmetric cryptography, the encryption operation and the decryption operation use the same key. The symmetric encryption algorithm is easy to operate, high in efficiency, relatively short in key, extremely difficult to decipher, and has good security and confidentiality. The security of the key is the decisive factor for the security of the computer network. Therefore, the secure transmission and storage of the key in the computer network security management is an important work content to ensure the security of the network information technology. In the symmetric encryption technology, a key is used for encryption and decryption to ensure the security of network information data, but it also has the disadvantage of not being able to realize the non-repudiation of data signature and information data. Symmetric encryption technology is fast and widely used in all walks of life.

Asymmetric encryption technology is different from symmetric encryption technology. Its main feature is that the encryption and decryption process uses completely different keys. Usually, it is divided into two keys: public key and private key. The public key is public and the private key is kept secret. The biggest advantage is that the receiver only needs to open the private key when the two sets of keys are decrypted, which can effectively realize the confidentiality of the data. Asymmetric encryption is flexible, but the decryption speed of the public key is relatively slow.

Node encryption technology is widely used in computer network security management. The premise of node encryption is peer-to-peer asynchronous or synchronous line. The encryption device at both ends of the node must be fully synchronized before it can be transmitted and encrypted. Its network manageability requirements. Higher. Node encryption is prone to transmission failure and loss during the transmission of information data. The node encryption technology requires that the routing information and the header are transmitted in a civilized form to ensure that the intermediate node has the ability to receive and process information. This method can effectively prevent the network attacker from stealing the analysis information data [3].

The link encryption technology encrypts the link in the network node to ensure the security of network information data transmission. The main feature of the link encryption technology is that the information data is encrypted before the information is transmitted, and then decrypted after being decrypted in the network node, and the security of the information data is realized in the repeated encryption and decryption by using keys of different natures. In general, in the link encryption technology, a piece of data information passes through multiple communication lines before reaching the receiver [4].

The end-to-end encryption technology adopts the data transmission mode from the start point to the end point in the encryption process. The data information transmitted is in the encrypted state before the final reception and decryption, and the decryption process is not performed in every link of the transmission process. Data is effectively secured during transmission. The end-to-end encryption technology has many advantages, the operation is relatively easy, the cost is low, the maintenance and use of the encryption design are relatively simple, and the user's data information transmission and reception requirements are met, and the transmission process is scientific and humanized. End-to-end encryption technology is worthy of widespread use and utilization, and continuously optimizes technology innovation during use.

## 6. Conclusion

With the continuous development of computer network technology, Internet information security issues will be more deeply valued, data security technology will be more in-depth research, and data security technology will inevitably penetrate into every detail corner of computer network information security management. The computer network information security has been comprehensively improved [5]. It is hoped that the data technology-related technology research and development personnel will continue to realize the theoretical innovation of information encryption technology, continuously accumulate experience in practice, and improve the various technical links of data encryption technology, which can make it provide more reliable and powerful guarantee for computer network data information security.

## References

[1] Geng Juan. Application of Data Encryption Technology in Computer Network Security [J]. Electronic Technology and Software Engineering: Information Security, 2014, 06, 12: 235.

[2] Wei Ruiliang. Research and application of data encryption technology in computer network communication security [D]. China University of Geosciences, 2013, 05, 01.

[3] Zhu Wenya. Research on Application Value of Data Encryption Technology in Computer Network Security [J]. Manufacturing Automation, 2012, 34(3): 35-36.

[4] Wang Yuxin. Application of Data Encryption Technology in Computer Network Security[J]. Proceedings of the 9th Shenyang Scientific Academic Conference (Economic Management and Humanities), 2012.

[5] Lian Shizhen. Application Analysis of Data Encryption Technology in Computer Network Communication Security [J]. Silicon Valley: Technical Application, 2011 (10): 162.