Application of data encryption technology in simulation software

Shaoqing He¹, Qian Wang²* and Xiaoting Li³

¹China Automotive Technology&Research Center Co., Ltd, Tianjin, 300300, China
²China Automotive Technology&Research Center Co., Ltd, Tianjin, 300300, China
³China Automotive Technology&Research Center Co., Ltd, Tianjin, 300300, China

* wangqian1994@catarc.ac.cn

Abstract. Due to the late start of China's industrial simulation software, the current virtual simulation market is basically occupied by foreign products, and the emerging forces are accelerating to enter. In order to help China occupy a field of simulation market, promote the research and development of simulation software, and ensure the security and stability of simulation network operation, this paper analyzes the definition, classification and principle of data encryption technology, and discusses the application of some encryption technology in simulation software [1].

1. Introduction
At present, the situation of network security is becoming more and more severe, and new threats to network security continue to emerge. The country’s political, cultural, economic, social, national defense security and legal rights and interests in cyberspace are facing various risks and challenges [2]. Among the many unstable factors in network security, the most prominent is the data security with the smallest granularity in the security and confidentiality levels involved in the operation of the application system. In order to improve the status quo of network security and improve the security of the data transmission process, this paper studies and discusses the definition, classification, principle and application of data encryption technology, and at the same time provides support for other related theories [3].

2. Computer network information security
With the advent of the "Internet of Everything" era, cyberspace, as the fifth space in addition to land, sea, air, and sky has formed network forms such as the Industrial Internet, the Internet of Vehicles, social networks, and the Industrial Internet. Due to the influence of various factors, computer network information security is difficult to effectively guarantee and it is prone to problems such as information loss, leakage, decryption, tampering, interception, etc., which poses a huge threat to the normal operation of all walks of life and even affects people. The normal use of information will endanger allergic personal and property safety and even national security [4]. These threats can be roughly summarized as the following:

2.1. The vulnerability of the computer network itself
The complexity, sharing, real-time and accessibility of computer networks determine the vulnerability of the computer itself. Among them, the advantage of the shared network feature is the rapid generation
and transmission of network information, which facilitates information sharing between users, but it has also become a breakthrough point in the theft of network information today. Moreover, the computers on the network always have to provide certain services to be able to communicate with other computers. The complex software system cannot be flawless and the fragility of the computer system and the computer network cannot be completely eliminated. As a result, due to the fragility of the computer itself, the network will inevitably produce corresponding harm when it is attacked.

2.2. Hacking illegal intrusion and attack
The rapid development of the network is generally positively related to the development of the capabilities of technical personnel. As the network becomes more and more complex, the attack capabilities of hackers are also advancing with the times. Hacking is the most serious security problem facing the network. In the first half of 2021, hackers attacked Colonial which is the largest fuel pipeline operator in the United States and forced the United States into a national emergency. In the end, Colonial paid the hackers 75 bitcoins. The purpose of most hackers' attacks is to extort money and some are because of hobbies. Some hackers feel that once they break a well-known website, they will feel a sense of accomplishment. Hacker intrusion methods are divided into active attack and passive attack. Active attack is a purposeful intrusion and attack that causes the other party's information to be leaked and data is lost. Passive attack is the theft and destruction of data without affecting the normal use of the computer by the user. Hackers' attack methods include, but are not limited to: stealing other people's information, exploiting firewall vulnerabilities, passing technical analysis, and passing emails. No matter what attack method the hacker uses, the result will reduce the user's sense of experience and even cause the user's property loss.

2.3. Other factors such as improper operation
Other factors that cause computer network insecurity include man-made factors, natural factors and some accidental factors. Human factors are the fundamental reason for the insecurity of computer information networks. At present, many people still do not have enough security awareness. They think that there is nothing too important in their electronic equipment or that there will be no such boring people coming to steal information, so they do not consider the operation of the machine from the perspective of security when setting the password or using it, which makes the criminals organic. It can take advantage of it. This situation has brought harmful effects to electronic equipment. There are also people with insufficient security technology capabilities, improper operations, incomplete test points during security testing before the system goes online and insecure server configuration when deployed online, which leads to vulnerabilities in the system, which also brings hidden dangers to the security of the WEB side.

3. Overview of data encryption

3.1. Definition and classification of data encryption
Data encryption refers to converting a message (plaintext) into an encrypted message (ciphertext) through an encryption algorithm and encryption key. Decryption refers to converting a ciphertext into plaintext through a decryption algorithm and decryption key. Its core is cryptography. The plain text is represented by M, the cipher text is represented by C, the encryption function is E, and the decryption function is D. The encryption and decryption process can be represented by mathematical formulas:

Encryption process

\[ E(M) = C \]

Decryption process

\[ D(C) = M \]
Encrypt and decrypt, and restore the original plaintext, so the following equation must be established:

$$D(E(M)) = M$$

Data encryption technology is divided into symmetric encryption technology and asymmetric encryption technology. The symmetric key of symmetric encryption technology has a small amount of calculation, fast speed and high security strength. Asymmetric encryption technology has irreversibility and is more secure than symmetric encryption technology. At present, several encryption technologies, such as DES, RSA, and ECC, which are widely used, are mainly discussed.

4. Common data encryption technology applications

4.1. Data Encryption Standard

Symmetric encryption technology is a shared secret key encryption technology. The sender of the message and the recipient of the message hold the same secret key to encrypt and decrypt the data during data transmission [7]. The popular explanation is that A transmits a message to B. A encrypts the plaintext and transmits it to B. After B obtains the ciphertext, it uses a common symmetric secret key to decrypt it. The information obtained by the eavesdropper from the transmission process is a bunch of garbled information. Diagram as shown in Figure 1. DES is a kind of symmetric encryption technology. DES uses a 56-bit key and an additional 8-bit parity bit to generate a maximum 64-bit packet size. If you want to try to break the secret key, it is easy. As long as you repeatedly try various secret keys by brute force, try up to the 56th power of 2 until it meets the requirements. When the DES algorithm first appeared, it satisfies the needs of system security. However, with the continuous development of computer system capabilities, the security of DES gradually decreases, and many encryption algorithms such as RSA appear.

4.2. Rivest Shamir Adleman

Asymmetric encryption technology is a public key encryption technology. The sender and receiver of a message hold different encryption keys and decryption keys during data transmission. In simple terms, asymmetric encryption means that A transmits a message to B. A uses B’s public key to encrypt the message and then transmits it to B. After B obtains the ciphertext, it uses its own private key to decrypt to obtain the real message, as shown in the Figure 2. RSA encryption is a kind of asymmetric encryption technology. The principle is to find two prime numbers, multiply the two, and then convert the binary algorithm, then calculate the Euler function of n, disclose n and e, and store the secret as d. Only authorized users can decrypt the ciphertext when they know d. The biggest disadvantage of RSA is its slow speed and obvious resource occupancy, so it is generally used for data encryption processing with small amounts of data, such as the login interface.
4.3. Elliptic Curves Cryptography

ECC is also an asymmetric encryption algorithm, which was proposed in 1985 and can be said to be a perfection on the basis of RSA. As the name implies, ECC is an encrypted public key method based on the cubic equation of the elliptic curve. It uses operations such as elliptic curve scalar multiplication and point addition, as well as the modulus algorithm of finite fields, to achieve fast digital signatures and signature verification[8]. The characteristic of ECC is that under the same encryption strength, its key length is much smaller than that of RSA, so it requires less storage space. See the following Table 1[9] for details:

| Break time | RSA key length | ECC key length | Key length ratio |
|------------|---------------|---------------|-----------------|
| $10^4$     | 512           | 106           | 5:1             |
| $10^{11}$  | 1024          | 160           | 7:1             |
| $10^{20}$  | 2048          | 210           | 10:1            |

At present, ECC has a wide range of applications and high security, and has become the focus of research in the field of e-commerce and military communication data transmission in recent years.

4.4. Examples of data encryption applications

Here is an example of data encryption used in this simulation software. In order to ensure that the actual content cannot be directly exposed after the message is intercepted by others during the data transmission of the system, the text content of the data is hereby encrypted. The following implementation content is to display each character array in the text after +1. For English, it is shifted backward by one position. For example, the original letter is "ab", and after encryption is "bc", the code is as follows:

```java
public class Test {
    static String text = "helloworld ";
    public static void sendMsg(){
        System.out.println("Before encryption:"+ text);
        StringBuffer stringBuffer = new StringBuffer();
        for(byte a: text.getBytes()){
            stringBuffer.append((char)(a +1));  //Encrypt every character
        }
        System.out.println("After encryption:" + stringBuffer.toString());
    }
    public static void main(string[] args){
        sendMsg();
    }
}
```

The result of the above code is: Before encryption: helloworld and After encryption: ifmmpxpsme.

This is just a simple encryption. The content of the encrypted field like RSA is more complicated, and there are basically no rules to follow, so it is popular. For example, the login user name is "admin1" and the password is "abc123". After encryption, the F12 front-end display is shown in Figure 3:
5. Conclusion

Now is the information age. If you want to solve the problem of computer network information security, the research and application of cryptography is indispensable. In addition to the above examples of DES, RSA, and ECC for data encryption, there are also node encryption, link encryption, and end-to-end encryption at the level of hierarchy [10]. With the rapid development of information networks, in order to expand the application range of data encryption technology in various fields, the research on data encryption technology does not stop there. In order to better respond to hacker intrusions, prevent virus attacks, and solve network information security, enterprises must actively apply data encryption technology [11] to create a more secure network information security environment for users.

References

[1] Yu Hao. Computer Network Security Research Based on Data Encryption Technology[J]. Network Security Technology and Application. TP393.08, 2021,(03):20-21
[2] Jiang Jianchun. Information Security Engineer's Course (Second Edition)[M]
[3] Yang Chao, Application of Data Encryption Technology in Computer Network Information Security[J]. China Science and Technology Information. TP393.08, 2021,(07):46-47
[4] Fang Zhouquan. Computer Application Based on Network Information Security Technology Management[J]. Technology Wind, TP393.08, 2021,(08):86-87
[5] Guo Xing. Computer network security and protection technology under the background of big data[J]. China New Telecommunications. TP393.08; TP311.13, 2021,23(06):143-144
[6] Bruce Schneier. Applied Cryptography[M]
[7] Yan Lihua, Li Yuxin, Shao Min. Research on the Application Value of Data Encryption Technology in Computer Network Security[J]. Network Security Technology and Application. TP393.08, 2021,(04):21-22
[8] Li Yu. Analysis and research of digital signature based on ECC algorithm[J]. Wireless Internet Technology. TP309, 2019, 16(12):110-111
[9] Yang Jiaxiong. Talking about Encryption Technology in E-commerce[J]. Computer Times. TN918.4, 2021,(04):38-41
[10] Tong Ying, Yao Huan, Zhang Liangjian. Computer Network Information Security Threats and Data Encryption Technology Research[J]. Network Security Technology and Application. TP393.08, 2021,(04):20-21
[11] Guan Tianwen. Research on the Application of Data Encryption Technology in Computer Network Security Management[J]. China Management Information Technology. TP393.08; TP309.7, 2021,24(07):173-175