Analysis and Comparison of Network Information Security Encryption Technology

Qiuyan Tian[1, a], Hao Kang[1, b], Ting Ai[1, c], Long Fei[2, d]

[1]Army College of Armored Force, Changchun, China

[2] Institute of Urban Environmental Sciences, Changchun Normal University, Changchun, China

[a] tqykali@163.com, [b] 29098545@ qq.com, [c] 65963974@qq.com, [d] flyflylong@163.com

Keywords: network; information security; encryption; password

Abstract*:* This article not only describes the network information security encryption mechanisms, but also analyzes the advantage of symmetric cryptography and asymmetric cryptography. It points out the problems which are noted in the application and compares the information encryption technology commonly used. Finally, this article prospects the development and application of information encryption technology.

1. Introduction

With computer technology, especially computer network of the rapid popularization and development, the global information technology has become a major trend of human development. The computer network has been widely used in the national defense military field, finance, telecommunications, securities, business and daily life. Especially the United States established the network war headquarters recently, and put forward ideas such as network centric warfare, which showed the importance of network technology. Network is easily attacked by hackers, crackers, malware and other illegal attacks because the computer connected with network diversity, the uneven distribution of terminal and network openness, connectivity and other features. So, how to ensure that important information is transmitted on the public network will not be theft, eavesdropping, forgery and tampering, which requires the use of cryptography to encrypt data processing. At present, the password technology has moved toward publicly from the diplomacy and the military field, and has developed into an interdisciplinary which involves many fields such as mathematics, computer science, electronics and communications, microelectronics technologies. Using cryptographic techniques can not only ensure the confidentiality of the information, but also can ensure the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting.

2. Analysis of information encryption technology

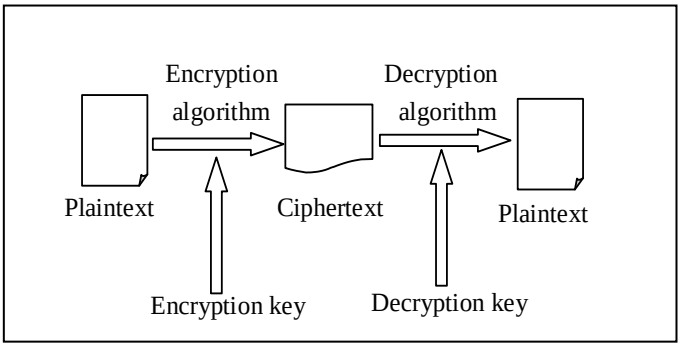

Figure 1: Data secret model.

Information encryption technology is the core technology which ensures network and

information security, and it is a proactive information security measures. The principle is the use of certain encryption algorithm, the plaintext can not be read directly into the text of the secret to prevent unauthorized users to access and understand the raw data to ensure data confidentiality. Plaintext into secret text is called encryption, and the secret text into plaintext is called decryption. The variable parameter of the encryption, decryption is called key. General data encryption model is like Figure 1.

Information encryption technology which based on key encryption algorithms are usually divided into different categories: symmetric encryption and asymmetric encryption technology.

2.1 Symmetric encryption

Symmetric encryption is also known as private key encryption technology, that's to say that the encryption key can be derived from the decryption key and in turn is also true. In most symmetric algorithms, the encryption and decryption keys is the same, these algorithms are also called a secret key algorithm or a single key algorithm [1]. The sender and recipient are required to agree on a key before they are in secure communications. Symmetric algorithm's security depends on the key. The key disclosure means that anyone on the message encryption or decryption. As long as communications are confidential, the key must be kept confidential. Therefore, the symmetrical algorithm is refers to the encryption and the decipher process uses the identical key, such as DES, 3DES, AES and other algorithms are symmetric algorithm.

The widely used symmetric encryption of the data encryption standard, is made by the United States, IBM.A block cipher algorithm which is published in 1977 by National Bureau of Standards is an iterative block cipher [2]. Although DES appears and then produced a number of conventional encryption algorithms, but DES is still the most important of such an algorithm. The entrance of the DES algorithm has three parameters: key, data, and mode. Key which is 8 bytes for 64-bit is the work key of the DES algorithm; Data which is also 8 bytes for 64-bit is to be encrypted or decrypted data; Mode is the mode of the DES algorithm, two; encryption or decryption.

DES algorithm has a very high security. So far, there is no more effective way to attack the outside of the DES algorithm in addition to the exhaustive search method. With the development of technology, as computer speeds increase, the DES key can add some length to achieve a higher level of confidentiality. However, this method is simple to use encryption and decryption speed, suitable for large amounts of information encryption .There are several problems: first, it can not guarantee and can not know the security key in transit, if the key leak, hackers can use it to decrypt the information, but also do bad things fake one; Second, assuming that each of the parties to the transaction with a different key, N side of the transaction requires N * (N-1) / 2 keys, difficult to manage; Third, data integrity can not be identified.

2.2 Asymmetric cryptography

Asymmetric encryption is also known as public key cryptography encryption technology. The encryption key Is different from the decryption key, and the decryption key can not be calculated according to the encryption key (At least within a long reasonable assumption time). The public key algorithm is called because the encryption key can open. That's to say that strangers can encrypt the message encryption key, but only with the corresponding decryption key can decrypt the information. However, to derive the private key from public key is very difficult. RSA, DSA and other algorithms are asymmetric algorithms, of which RSA is most widely used, not only can also be used to encrypt the digital signature.

RSA is the first comprehensive public-key cryptosystem which was put forward by Rivet, Shamir, and Adelman in 1977. RSA algorithm is based on Euler's theorem in number theory, the mathematical principle is to break large numbers into a product of two prime numbers, encryption and decryption using two different keys are actually two large prime numbers, with which a prime number multiplied with the plaintext can be encrypted cryptograph; with another prime number by multiplying with the cryptograph can be decrypted to restore the plaintext. It is very difficult to use a prime number to find another prime number, so you can get a higher level of confidentiality.

RSA system is the most typical method in public key system, most products and standards which

are encrypted and digitally signed by public key cryptography use RSA algorithm. The major advantages of RSA method are simple in principle, easy to use. However, with the progress and improvement of the decomposition method of large integers, computer speeds increase and computer network development, security of RSA encryption and decryption of large integers requires more and more. In order to ensure the security of RSA, the number of bits of its key has been increasing, for example, now generally believed that RSA needs the word length of more than 1024 have security. However, the speed of encryption and decryption are greatly reduced by the key length increases, hardware has become more and more unbearable, which brings a heavy burden for the use of RSA applications, especially for a large number secure transactions of e-commerce, making its application more and more constraints.

2.3 Hybrid encryption based on DES and RSA

In encryption, decryption processing efficiency, DES algorithm is better than the RSA algorithm [3]. Because the DES has only 56-bit key length, you can use the software and hardware to tell processing, when you implement software, encryption speed can reach several megabytes per second, for a lot of information encryption; As a result of the RSA algorithm is the calculation of large numbers, making the fastest of RSA is much slower than DES, either software or hardware, the speed of RSA has been a defect, usually only for a small amount of data encryption. In key management, RSA algorithm is more advantageous than the DES algorithm. Because the RSA algorithm can be open to the public distribution of encryption keys, the update of the encryption key is also very easy, different communication objects only keep secret for their own decryption key. DES algorithm secretly distributes the key before communication, Key replacement is difficult, DES need to have custody of a different key for different communication objects, in the signature and certification, DES algorithm can not be achieved on the principle figures from Visa and authentication, but the RSA algorithm can be easily digital visas and identity authentication. Sender's private key encrypted data can provide the identity of the sender authentication, recipient private key encrypted data can provide authentication of the identity of the recipient [4].

In the hybrid DES and RSA encryption algorithm, using DES encryption of large amounts of data will not affect the overall efficiency of the system. DES with RSA algorithm for key encryption can be open, and RSA's encryption key can be exposed, so the whole system needs only a small amount of RSA secret decryption key. The encryption system can not only play fast DES encryption algorithms, security and good benefits, but also easy to play the RSA algorithm key management advantages.

3. Other digital encryption technology

3.1 Digital Summary

Digital abstract, also known as digital fingerprinting, Secure Hash coding or MDS, use One-way Hash functions encryption algorithm to encrypt the arbitrary length message, Summary into a string of 128 bits of cryptograph, this cryptograph is called digital digest or message digest [5]. Digital digest is a unique piece of data corresponding to the value, the so-called one-way can not be decrypted. The different data has its different summary, and the same data has the same summary. So the summary as the fingerprint of data confirms whether the message is really the body.

3.2 Digital Signature

The so-called digital signature is some data attached to the data unit, or the password transform to the data unit, this data or transform allows the recipient to confirm the data unit source and the integrity to protect data, to prevent people (such as receiver) to false. It is a way to sign the message of the electronic form, and a signed message can be transmitted in a communication network. Based on public key cryptography and private key cryptography can obtain a digital signature, at present the digital signatures is mostly based on public key cryptography.

Ordinary digital signature algorithm includes RSA, ElGamal, Fiat-Shamir, Guillou-Quisquarter,

Des / DSA, elliptic curve digital signature algorithm and finite automata digital signature algorithm etc. Special digital signature, including blind signature, proxy signature, group signature, undeniable signature, fair blind signature, threshold signature, the signature with message recovery, etc., it is closely related to the specific application environment. Obviously, the application of digital signatures related to legal issues, the federal government based on a limited domain of the discrete logarithm problem has developed its own Digital Signature Standard (DSS).

3.3 Digital Envelope

The so-called digital envelope is the message sender's public key with the receiving end, which encrypts a Symmetric communication key, the formation of the data is called a digital envelope [6]. This digital envelope is sent to the receiver, only the designated receiver can just open the digital envelope own private key, to get the symmetric key, because the receiver can be used to interpret the password sent to communicate information. It's like in life, a key in an envelope, to mail each other, the other received a letter, remove the key to open the safe.

The digital envelope unifies the symmetrical key and the asymmetrical key ingeniously. It synthesized the two kinds of technology and provides the advantages of both.

3.4 Digital Certificates

Digital certificate is a series of data which sign all identity information in Internet communication, provides a way to verify the identity On the Internet its role is similar to driver's license or ID card in daily life. It is issued by an authority-CA, also known as certificate authority, CA is an authority which is responsible for issuing certificates, certification, and management. It is necessary to formulate policies and concrete steps to verify, identify the user, and user certificates signed to ensure that the certificate holder's identity and public key ownership.

Thus, the construction of Certificate Authority (CA) Center, to develop and regulate e-commerce market is an essential part. To ensure the transmission of information between users in online security, authenticity, reliability, integrity and non-repudiation, this not only need to verify the authenticity of the user's identity, also need to have an authoritative, impartial, uniqueness of the body which is responsible for issuing to all the main e-commerce and management in line with national and international standards for secure electronic transaction protocol of electronic business security certificate.

3.5 Digital Watermarking

In recent years, in addition to traditional cryptography, the rise of a new information security technology, an information hiding technique, is also known as digital watermarking technology. The information which should be kept confidential hides in the audio-visual data by using various signal processing methods, after unauthorized users intercepted a secret file ,he can only read the file contents of the carrier, and not realize that it contains confidential information, or even know that it contains confidential information ,but can not be deciphered.

Message Authentication and access control technology is equivalent to the information to be protected with a layer of the door, to prevent unauthorized users from close and use. Password-protected information technology is to change into a meaningless content which unauthorized users can not understand. The information hiding is to protect the information hidden in the multimedia carrier, so unauthorized users will not notice the existence of hidden information or can not detect the information. Information hiding technology not only prevents unauthorized users from extracting the watermark information, and can avoid the attack. Traditional cryptographic techniques can be used to protect digital works, but the media once decrypted, you can spread freely, and copy; at the same time, due to the complexity of the decryption algorithm, it is difficult to meet the requirements of real-time, information hiding just to overcome these shortcomings.

4. Summary

With the development and the popularity of computer and Internet, factors to threat information

security are more and more. Now there are several ways to protect information security and information encryption technology, but there is no absolute good or bad in a variety of encryption technologies. To use the appropriate encryption algorithm in various occasions can receive good results. Only by understanding the encryption algorithm, and on this basis to make the appropriate improvements, this can find a suitable encryption algorithm which uses in secure communications of military field. Meanwhile, with the deciphering method, hardware technology, cryptographic algorithms, applications and standardization is also constantly evolving. Quantum cryptography, passwords and other neural network research and application of new password show that cryptography has a strong vitality and broad prospects, which plays a good protection to information security.

Acknowledgments

The article gets Jilin educational fund projects support, Project Numbers: Ji Jiao Ke He Zi [2011] No 197.

References

[1] Qing Sihan, Cryptology and computer network security, Tsinghua University Press, 2014.

[2] Li Lian, “The DES Encryption Algorithm in InformationSecurity,” Modern electronic technique, vol. 200, pp. 118–120, May 2013.

[3] Li Ming, Wang Yong, Gu Dawu, “An Identity-based Authenticated Group Key Agreement Scheme,” Computer Engineering, vol. 30, pp. 1–2, Otcober 2015.

[4] Xu Qingzheng, “Public key infrastructure (PKI) synopsis,” Data Communication, vol. 218, pp. 11–12, June 2014

[5] Yang Yang, Gao Yin-jing, Tang Fu-hua, “Novel watermarking embedding algorithm for AFIS based on secure network transmission,” Computer Applications, vol. 24, pp. 70–72, December 2015.

[6] Su Gui-ping, Yao Xu-chu, Lu Shu-wang, “Random mumber generation method of information security system,” Computer Applications, vol. 25, pp. 837–839, April 2014.