Study on data encryption technology in network information security

Jianliang Meng, Tao Wu [a]

School of North China Electric Power University, HeBei 071000, China

[a] iversonwtao@163.com

Keywords: Network, Information Safe, Encryption technology, Encryption algorithm Application.

Abstract. The progressive development of computer technology, network information security trend to increasing tensions, as well as all kinds of theft, tampering with and destruction of social development have a higher level of network and information security requirements. Data encryption is to protect the core technology of network information security technology, reduce the level of computer attacks, parsing, to some extent, improve the security of data transmission, and ensure the integrity of transmitted data.

1. Objective

The rapid spread of Internet on a global scale and popularity, making the exchange of information and data transmitted over the network rapidly increasing, so for network information security issues become increasingly prominent, and study on encryption for all kinds of information is particularly important. Information on computer encryption, encrypt or decrypt transform is implemented by a key control. Key is a randomly selected user in accordance with a cipher system, it is usually a random string, is the only parameter control transformation of plaintext and ciphertext.

Data encryption is the original digital information through encryption system (clear text), an encryption algorithm transforms plaintext completely different digital information (redaction) process.

2. Data encryption techniques

2.1 Data encryption techniques

Mainly in computer data encryption technology as the core, provides the corresponding algorithms to achieve the rapid transformation of plaintext, ciphertext, and stable encryption, plaintext into ciphertext through the algorithm, only under the conditions in the key match, data can only be read to avoid attacks, illegal interception, transmission of computer information security.

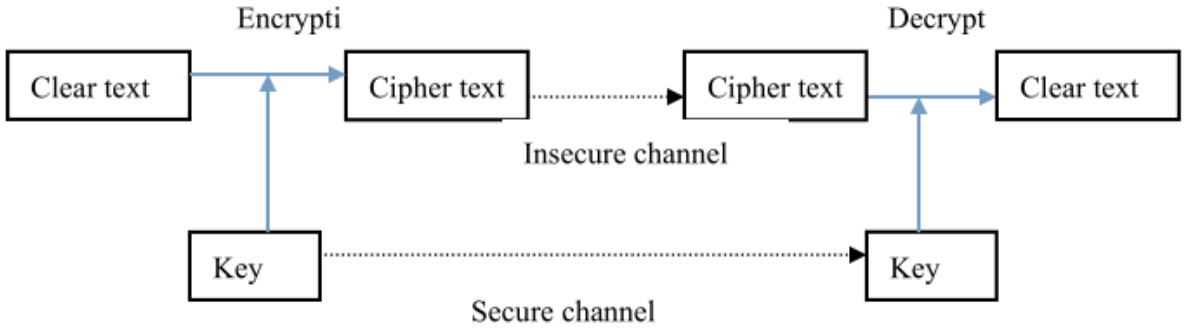

Figure 1 General model of data encryption

2.2 categories of data encryption technology

Data encryption techniques are mainly divided into encrypted data encryption and data storage. Encryption technology of data transmission is the transmission of data stream encryption, commonly used link encryption, encryption and end-to-end encryption of the node 3 ways [3].

Link encryption: usually called network layer encryption link encryption, mainly for the protection of data transmitted between communicating nodes, regardless of the source and host, the password for the encryption and decryption by placed on the line device.

Nodes are encrypted: improvement of link encryption is. On the protocols of the transport layer encryption, node a and node connected to cryptographic devices, cipher text is decrypted and re-encrypted in this device, plaintext, not through nodes, overcoming link encryption weaknesses in node vulnerable to illicit access.

End to end encryption: encryption at the application layer. Data in the transmitter are encrypted, and decrypted at the receiving end, intermediate nodes do not appear in clear text. Information is made up of header and the message, message in order to transfer information header for routing information, since transmission involves routing, link encryption, respectively, are required to encrypt the message and header. But in the end-to-end encryption, to encrypt the message, instead of the header encryption. In the transmitter and the receiver have the encryption, decryption device, and are not decrypted messages any node in the Middle, therefore, does not need password devices, compared with link encryption, but reduces the number of password facility.

3. Data encryption algorithm

There are many kinds of data encryption algorithm, according to the development process, experience the classical password, symmetric key cipher and asymmetric key cipher stage.Classical ciphers are alternative encryption, encrypted replacement; a symmetric encryption algorithm such as DES, AES; asymmetric encryption algorithms are RSA, DSA, and elliptic curve (ECC).

3.1 the DES (data encryption standard)

DES is an encryption algorithm for binary data, is likely to be the most widely used key systems, in particular in the protection of the security of financial data. In General, automatic teller machines using DEA.

Weaknesses of the DES algorithm is unable to provide adequate security, because its only 56-bit key length.

3.2 AES

With the development of symmetric ciphers, DES data encryption standard algorithm due to the smaller key lengths (56-bit), does not meet the demands of today's distributed open network for data encryption security. Moved the AES as the United States data encryption standard has been widely applied to various fields. Overall, the AES as a new generation of data encryption standard brings together a strong security, high performance, and high efficiency, ease of use and flexibility advantages.

3.3 RSA

RSA algorithm is the first that can be used both for encryption and digital signature algorithm, is the most widely used public-key cryptography. It resists all known cryptographic attacks so far has been IS0 recommended standards for public key encryption. Its security is the difficulty of factorization based on large prime numbers, prime factorization problem is a famous problem in mathematics, there is no effective ways of solving them, and so you can ensure the security of RSA algorithm.

RSA algorithm has the advantage of large key space, the disadvantage is that encryption is slow, if used in conjunction DES and RSA, you just make up for the disadvantages of RSA. DES for plaintext encryption, RSA for the DES encryption key. Due to the speed of DES encryption, suitable for encrypting long messages, and the RSA DES key distribution problem can be solved.

3.4 DSA

DSA are generally used for digital signatures and authentication. DSA is a variant of Schnorr signature and ElGamal algorithms, United States NIST as DSS (DigitalSignature Standard). DSA is based on limited integer field of the discrete logarithm problem, its safety compared with the RSA.

DSA digital signatures and authentication, the sender uses its own private key to sign the document or message, and recipients receive the message using the sender's public key to verify the

authenticity of the signature. DSA and RSA is different in that it cannot be used for encryption and decryption, or key exchange, only used to sign, it is a lot faster than RSA.

3.5 elliptic curve (ECC)

Elliptic curve cryptography ECC (Elliptic Curve Cryptography) is a more secure public key systems, algorithms to achieve better performance. Its security is based on the difficulty based on the elliptic curve discrete logarithm problem, its scope at present are mainly fast encryption and decryption, digital signatures, authentication, mobile communication and other fields[2].

For RSA, it's safe to use a key strength depends on its length, but along with the rapid development of computer technology, 512-bit length of the key is no longer secure, and 2048-bit length of the key in the coming period of time will be considered to be safe. ECC encryption strength under the same premise, the required key short, ECC and RSA/DSA safety is given below, compares the results as shown in Figure 2 and table 1[1] (which is generally believed to decipher for MIPS years indicates that the cipher is secure).

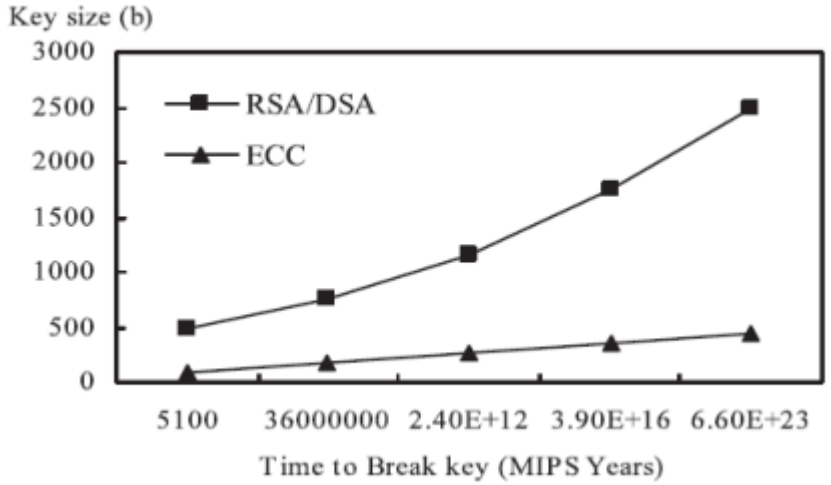

Figure 2 RSA/DSA safety comparison with ECC

Table 1 RSA/DSA and ECC key length comparison

Break time	RSA/DSA Key length	ECC Key length	Secret key length ratio
$1.0*10^4$	$5.12*10^2$	$1.06*10^2$	$4.8/1$
$1.0*10^8$	$7.68*10^2$	$1.32*10^2$	$5.8/1$
$1.0*10^{12}$	$1.024*10^3$	$1.6*10^2$	$6.4/1$
$1.0*10^{20}$	$2.048*10^3$	$2.1*10^2$	$9.4/1$
$1.0*10^{78}$	$2.1*10^4$	$6.0*10^2$	$35.0/1$

Table 1 shows that RSA/DSA when key length of 1024 bits is required in order to meet security needs, and ECC 160 bits is sufficient to meet security needs. And Dang key length increased Shi, ECC password algorithm of security strength to than RSA and DSA of security strength increased fast have more, for example key length for 210 bit of ECC password algorithm to than 2048 bit of RSA password algorithm and DSA password algorithm security, at RSA password algorithm and DSA password algorithm of key length from 1024 bit increased to has 2048 bit, and ECC password algorithm of key length just from 160 bit increased to 210 bit. Therefore, relative to the RSA/DSA and other public key cryptography, ECC has high strength, small operations, key length shorter, faster, less bandwidth required and so on[1].

ECC features make it will replace RSA, becoming the most important mainstream public-key encryption algorithm.

4. the development of encryption technology

New encryption methods are constantly forming in scientific inquiry, in which encryption with new knowledge and exploration, innovative encryption technology developed in recent years, showed several development mechanisms [5].

4.1 Quantum Cryptography

Using single-photon principle in optical fiber level key management and encryption.

Narrow sense of quantum cryptography is also known as quantum key distribution, remote communication can be provided unconditionally secure key agreement methods. Its security is based on the principles of quantum mechanics (unknown quantum state cannot be cloned collapse, quantum measurement and quantum uncertainty principle), do not rely on third party eavesdroppers computing power and storage capacity, thus meaning unconditionally secure cryptography can be achieved[3]. Quantum Cryptography is the most mature technology development in the field of quantum information, combined with quantum cryptography, and "a secret" password system can implement unconditionally secure secret communication system.

4.2 the DNA code

DNA password is the password for the new technologies, is one of the potential alternatives to traditional password techniques. Characterized with DNA as the carrier of information through modern biotechnology, mining DNA the inherent advantages of high density, high parallelism, encryption, authentication, and signature and cryptography features.

Because of its security does not rely on difficult mathematical problems, DNA code in a future powerful quantum computers and computers will not be obsolete, but compared with quantum cryptography, DNA code is more suitable for high density data storage[2].

4.3 chaotic encryption

Chaos is a seemingly random movements, in a deterministic system appears similar to the random process. Chaos has sensitive dependence on initial conditions and parameter. By selecting the parameter as keys, chaos can be used to design a cipher system.

5. The application of data encryption technology

5.1 digital signatures

Digital signature using the RSA algorithm, the sender of data using its own private key to encrypt data, recipient using the sender's public key to decrypt because strict correspondence between the private and public keys, using one of the only other solution, ensure that the sender cannot deny sending the data.

5.2 database encryption

Database system as the core of modern information systems. Current database security in addition to access control, the most effective way is to encrypt the data stored within the database [2]. Multistage chaotic system generating chaotic key stream to a high intensity, characteristics of high efficiency, more in line with the characteristics of database encryption.

5.3 key protection

For the protection of personal information. Key protection: when data transmission is, the first public key is used to encrypt the transmitted information, user accepts data in the process, decrypted using the private key, in the presence of key, escort run data, not only to avoid the attacker to steal data in the path [2], and has the effect of the security and integrity of information transfer.

5.4 USB Security Key

Hardware USB Key is a USB interface device. Its built-in MCU or smart card chips, there are some storage space, you can store the user's private key and digital certificate, public key algorithm using the built-in USB Key authentication of user identity [5]. Due to the user private key in the lock,

in theory, cannot be read with any way, guarantee the security of user authentication. Mainly used in banking transactions system.

6. Conclusion

With the rapid development of computer and network applications, more and more unsafe, and data encryption technology of network information security provides an effective means of protection, one should increase the intensity of the study on data encryption technology. While information security tasks are manifold, involving not only data encryption, intrusion detection, anti-virus software and other security technologies to enhance people's awareness of information security, and improving information security management system and relevant laws and regulations, it is also very important.

References

[1] Li Dianwei, Wang Zhengyi, Zhao Junge. Safety analysis of elliptic curve cryptography [j]. With the development of computer technology. 2012, 22 (4): 228-234.

[2] Zhao Junmei. Discussion on the application of data encryption technology in computer security [j]. Innovation and application of technology. 2014 (19): 66.

[3] Yang Yan. Discussion on network attack and defense techniques [j]. Information and communication. 2013 (7): 133-134.

[4] Luo Huilan. Data encryption technology and its application in the field of computer network security [j]. Information security and technology. 2013, 4 (11): 64-65.

[5] Cai Fangbo. Analysis and application of encryption algorithm [j]. Network security technologies and applications. 2014 (4): 67-71.