Application of Public Wife Key Encryption Algorithm in Network Information Security Center

Lin Xinping[1,a,*], **Liu Anping**[2]

[1]Computer Science Department, Shantou Polytechnic, Shantou, Guangdong, 515078, China

[2]huizhou Secrecy Administration Bureau, Huizhou, Guangdong, 515000, China

[a] email: xplin@stpt.edu.cn

*corresponding author

Keywords: Information Security, Public Key, Encrypted Transmission

Abstract: With the development of information society and e-commerce, people pay more and more attention to information security. The security of network data transmission has become a concern. Data encryption has become a topic of international information communication. Based on the public key encryption algorithm, this paper discusses the information security and practical problems in the Internet environment.

1. Introduction

Although cryptography has a long history, but only after the emergence of number theory, especially after the emergence of number theory, cryptography has a high complexity of cryptography, and the public key encryption algorithm came into being in a short time. It was in 1976, Herman et al. The public key encryption algorithm is given [1]. In modern cryptography, there are two encryption methods: one is the encryption of symmetric key cryptosystem, the other is the encryption of symmetric key cryptosystem. The encryption of the key, also known as private key encryption, means that the issuer and receiver of the information use the key to encrypt and decrypt the data. Its advantage is confidentiality, suitable for big data encryption, but key management is difficult. It is also called individual key cryptosystem, that is, the same cryptosystem of encryption key and decryption key. The secrecy of their cipher depends on the secrecy of the key. In order to ensure the security of the key system, the encryption algorithm must be complex enough, and the key must be kept secret, and there is enough space to store the key, so that the attacker can not get the original text even if he extracts the key text and knows the encryption algorithm. The most representative symmetric key cryptography program is the data encryption system des, which was established by the Standards Bureau of China in 1977. When information is transmitted through the network, asymmetric key cryptography algorithm has irreplaceable advantages over symmetric key cryptography algorithm [2]. The service sub supplier of online e-commerce at home says that in general, at least in the open network and hundreds of customers can access the trunking and transaction, such as fruit access trunking and symmetric secret key and secret, that is, Yaoshang building will need to provide each The guest's door points to a secret key, and when the password pass is lost, there must be a very secure one-way pass. However, in asymmetric key encryption algorithm, this is unnecessary. The merchant simply presents a pair of keys and opens them. Customers only need to use the public key provided by the merchant to encrypt the information, and then they can transfer the information to the merchant safely. Although it is not a symmetric key cryptography algorithm, it has an optimal point [2]. Symmetric key algorithm is irreplaceable, and it also has a fatal weakness, that is, the speed is too slow. Therefore, in fact, we usually combine the two algorithms.

DOI: 10.25236/ictmic.2020.076

Table 1 Comparison of public chain, private chain and alliance chain

	Public chain	Private chain	Alliance chain
Centralization	No center	Centered	Multicenter
Participant	All	Control center decision	Preset members
Bookkeeper	All participants	Control center decision	Consult
Trust mechanism	Proof of work	Endorsement on its own initiative	DPOS
Advantage	To the center, to trust	Low energy consumption	Can control permissions
Shortcoming	Limited trading capacity	Access node Limited	Can't solve the information problem completely

2. Symmetric Key Cryptosystem

Key encryption can also be called special key encryption or general key encryption, that is, both sides of data receiving and sending must use the same key to encrypt and decrypt plain text. Symmetric key encryption algorithms are des, 3DES, idea, FeAl, blowfish and so on[3]. DES is the German Engma cryptograph captured by the allies in the Second World War. Of course, it's more complicated and severe. The old and powerful encryption algorithm is widely used, it is quite famous. The algorithm itself is called DEA (data encryption algorithm). DES is the most commonly used symmetric compression method. Des keys are 56 by 64. In order to improve the fastening strength, the 3DES compaction method is developed. There are two types of modules in symmetric key encryption system. One is the central encryption module, the other is no central encryption module.

Table 1 Performance comparison of PID parameter optimization method in second order system

Algorithm	K_P	K_I	K_D	ITAE	Iteration times
PSO	33.6917	0.1662	38.8852	1.0581	94
GA	33.7908	0.1665	38.5647	1.0584	77
Algorithm in this paper	33.0957	0.1662	38.2064	1.0580	64

2.1. Centralized Encryption Mode

The central model means that there is an independent center, and every user trusts him[4]. This center is responsible for assigning keys to each user and managing all user keys stored in the store. If any user's key has to be compromised, the change center will void the key label. When there is secret communication between users, the management center confirms that the key of the other party is the current user, and the key of the other party is invalid. The central encryption mode has the following three characteristics. Because the key is randomly generated, it is impossible to determine which user, so the key management center needs to save the mapping relationship between the key and the user. The risk of tampering and key leakage B. in the secret communication between two users, the key management center needs to dynamically verify the validity of each other's key. The performance of password management center is degraded because of the failure of offline secret communication. C. the number of key assignments and users is linear. If there are n users, you can assign n keys, and each user can keep one key. The key management center needs to ensure that each user and their corresponding relationship remain critical. Due to the frequent need to confirm the legitimacy of each key online, it is also time-consuming and inappropriate for large-scale public service areas. This mode is better known than the path application field of magnetic stripe card. In fact, it has become the standard application of bank system password. It is widely used in almost all domestic and foreign banks[5]. Most of the user's key memory, in order to prevent offline transactions from becoming possible, the parent's lock-in mechanism has been imported with the electronic wallet password application. This mechanism is based on the user's inherent identification, that is, the parent key directly generates the card number of the key. The parent key is indeed stored on all clients and all devices. The user key is not saved at this time. When the user uses that, please confirm the key and the user. When wiring, the local key can be calculated according to the user's key, so that the credit card number and the user can be separated locally.

2.2. No Central Encryption Mode

In the decentralized mode, two users negotiate to obtain the shared key. In order to prevent the key compromise of the third user from affecting the two users, the key between each two users must be independent of each other. In order to prevent key leakage, when communicating with two users in secret, they encrypt the data directly to share the password. Please do not use it. The centerless encryption mode has the following three characteristics[6]. The number of negotiated key protocols increases with the number of users. B. each user must maintain a shared key with other users. If there are n users, each user needs to keep the N - 1 key. The key negotiation between each user is flexible and unaffected by other users. In order to increase the number of negotiations according to the number of users, each user must manage most of the shared keys, which is not suitable for large-scale users.

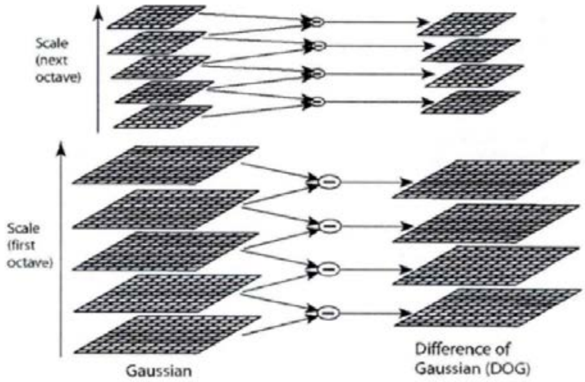

Figure 1 generation of Gauss difference pyramid

3. Asymmetric Key Cryptosystem

Different from the above-mentioned encryption methods, asymmetric key encryption system uses several mathematical theoretical problems to realize. Asymmetric key encryption algorithm is also called public key encryption algorithm. Two pairs of secret key and public key are used. You can make your private keys public, but you have to make sure that. Private key and public key are closely related. Information encrypted with public key can only be decrypted with secret key[7]. The public key algorithm does not need an online key server, and the key distribution protocol is simple. In addition to encryption, the public key system can also provide digital signatures. RSA is the most widely used public key encryption algorithm. RSA was developed by Ronald L. riest, ady Shamir and Leonard M. Adleman in 1977. RSA consists of three abbreviations. RSA uses public and private keys. If you encrypt with one of them, you can use it to decrypt other things. The key length is 40-2048 bits. When encrypted, the plaintext is divided into blocks. The size of the block is variable, but cannot exceed the key length. Convert to ciphertext block of the same length as the key. A longer key has a greater encryption effect and a better encryption and decryption cost. Therefore, the compromise between security and performance is usually considered. In general, 64 bit is more appropriate. RSA's more famous application is SSL. In the United States and Canada, SSL uses the 128 bit RSA algorithm. Due to export restrictions, it is usually used in other regions, including China. Public key method is slower than private key method. Therefore, the combination of public and private key technologies is often used to achieve optimal performance [8]. That is, the public key technology is used to support the private key between communication, and the private key is used to encrypt and decrypt the data actually passed.

4. Comparison between Symmetric Encryption Algorithm and Asymmetric Encryption Algorithm

First, we need to understand the current encryption technology. Data encryption technology can be divided into two types: symmetric encryption (private key encryption) and asymmetric encryption (public key encryption). Symmetric encryption is usually represented by data encryption standard (DES) algorithm. Encryption and decryption keys are different. It is necessary to disclose the encryption key to keep the decryption key secret. Please consider the operation mode of your website again. The three-tier structure we usually use is divided into three parts: database, website server and client. In the process of using, the client sends a request to the server, the server queries the corresponding data in the database according to the user's request, and returns to the client to generate a web page to complete the interaction process. Finally, let's take a look at the encrypted transmission process of important data. The encrypted data sent by the website is divided into two parts: server-side data encryption and client-side data encryption. In the encryption on the server side, the server first encrypts the core data to the ciphertext, and then sends the ciphertext to the network client [9]. The client decrypts the ciphertext to get the plaintext. If the client is encrypted, the process is the opposite. The client encrypts the core data sent and sends it to the server. The server decrypts the ciphertext for plaintext. Based on the above analysis, please compare the advantages and disadvantages of different encryption technologies. When using symmetric encryption algorithm, you need to select the same encryption and decryption key. Used for data encryption and decryption. The advantages of using this encryption technology are high encryption speed and high data encryption strength. Because the encryption key is the same as the decryption key, the security of the key must be strictly guaranteed. Otherwise, once the key is stolen, hackers can easily extract the ciphertext, or they can use the key to forge data. When using asymmetric encryption algorithm, the server and client must first calculate the public key and private key. When encrypting, use the public key of the other party to encrypt the data. After receiving the ciphertext, the other party uses its own private key to decrypt the data. The advantage of this method is that the encryption key and the decryption key are separated, and the ciphertext cannot be decrypted with the encryption key. Therefore, the encryption key can be disclosed on the network. This method can use each key pair to perform the calculation and provide the public key to the other party. These algorithms are developed based on mathematical problems, so asymmetric encryption algorithm also has its inherent shortcomings. In terms of quantity calculation, RSA is slower than des. RSA is always flawed. Generally only used for a small amount of data encryption.

5. Conclusion

Now there are two main branches of data encryption: symmetric key encryption and asymmetric key encryption. Symmetric key encryption algorithm is actually the traditional encryption method developed to today. After DES algorithm, there are some new algorithms, such as ideas, but most of them are used to make up for the shortcomings of Des short key length [10]. For encryption methods, it is similar to des because it uses transformation and replacement methods for scrambling the original data. Compared with thousands of years of research history of symmetric key encryption system, asymmetric key encryption system is a new encryption system. In addition to the military cryptosystem, there are business secrets of the military cryptosystem. In practical applications, symmetric key algorithm and asymmetric key algorithm need to cooperate with each other to complete the data encryption requirements in the Internet network environment.

References

[1] He Simeng, Yang Chao, Jiang Qi,. Deduplication on Encrypted Data Based on Zero-Knowledge Proof and Key Transmission. Journal of Computer Research & Development, 2018.

[2] Amit Kumar Singh, Zhihan Lv, Seungmin Rho,. IEEE Access Special Section Editorial:

Information Security Solutions for Telemedicine Applications. IEEE Access, vol. 6, pp. 79005-79009, 2018.

[3] Eldin S M S. Encrypted gray image transmission over OFDM channel for TV cloud computing, vol. 20, no. 11, pp. 1-12, 2017.

[4] Ahmed El Shafie, Asma Mabrouk, Kamel Tourki,. A Secret-Key-Aided Scheme to Secure Transmissions from Single-Antenna RF-EH Source Nodes. IEEE Wireless Communication Letters, no. 99, pp. 1-1, 2017.

[5] Vincent Y. F. Tan, Si-Hyeon Lee. Time-Division Transmission is Optimal for Covert Communication over Broadcast Channels. IEEE Transactions on Information Forensics and Security, no. 99, 2017.

[6] Walid El-Shafai, El-Sayed Mahmoud El-Rabaie, M. M. El-Halawany,. Security of 3D-HEVC Transmission Based on Fusion and Watermarking Techniques. Multimedia Tools and Applications, 2019.

[7] Tan D, Jingzhao L I, Yang D, et al. Optimization Strategy of Information Interaction Maximum Flow Transmission in Vehicle Ad Hoc Network, 2017.

[8] Elisa C. Baek, Christin Scholz,. Matthew Brook O’Donnell, The Value of Sharing Information: A Neural Account of Information Transmission. Psychol Sci, vol. 28, no. 3, pp. 095679761769507, 2017.

[9] Axel Dreher, Sarah Langlotz, Silvia Marchesi. Information Transmission And Ownership Consolidation In Aid Programs. Economic Inquiry, vol. 55, 2017.

[10] Zaheer Khan, Zeeshan Pervez, Abdul Ghafoor Abbasi. Towards a secure service provisioning framework in a Smart city environment. Future Generation Computer Systems, vol. 77, 2017.