ALGORITHM DESIGN OF SECURE DATA MESSAGE TRANSMISSION BASED ON OPENSSL AND VPN

SHI-HAI ZHU
Department of Computer and Information Engineering, Zhejiang Water Conservancy and Hydropower College
Hangzhou, Zhejiang Province 310018, China
E-mail: yyzz98@163.com

ABSTRACT

In order to solve the safety problem that remote or mobile users can perform secure data transmission among different computers via enterprise internal network, conventional approach is to establish VPN connection. The transmitted data via VPN network must be encrypted so as to ensure that illegal users are unable to read them, therefore data security of VPN network depends entirely on the strength of the adopted encryption algorithm. In this paper we propose a secure data transmission algorithm based on OpenSSL and VPN. It combines both the characteristics of asymmetric password system and symmetric crypto-system, and provides a good and fast way for the safety of information transmission. On the whole, the algorithm has such advantages as simple principle, higher security, and so on. Meanwhile it is more convenient to be implemented by hardware and software, better meeting design criteria of encryption algorithm. Besides, our practice in water conservancy practice shows that the adoption of this algorithm can well realize fast and secure information transmission.

Keywords: *OpenSSL, VPN, Digital Signature, Encryption Algorithm, Decryption Algorithm.*

1. INTRODUCTION

When remote or mobile users want to browse the information stored on the private networks of their enterprises while they are on business or at home, building dial-up VPN connections is an ideal choice. In order to effectively improve network security, encryption-decryption algorithm and digital signature technologies have been widely used. Cryptography [1, 8] is a new study aiming at data encryption, decryption and relevant transformation. Cryptography has been widely studied at home and abroad and a lot of practical encryption algorithms, such as 3DES [2], AES, RSA [3] and so on have been put forward. Various properties of the encryption system are mainly determined by the cryptographic algorithm. Encryption system is generally divided into two types: symmetric and asymmetric crypto-systems. Both symmetric and asymmetric key encryption system have their own advantages, but there are some insurmountable problems at the same time [4, 9]. In this paper, we propose a secure data transmission algorithm based on VPN and OpenSSL. Our practice in water conservancy engineering practice shows that users can use this algorithm to transmit data message securely.

This paper is structured as follows. Section 2 describes the secure technology of VPN. Section 3 gives the construction procedure of software VPN server and discusses its advantages. In Section 4, we analyze the encryption algorithms of AES and ECC, and make a brief introduction of digital signature and OpenSSL. Section 5 describes the secure data transmission algorithm and its application in water conservancy engineering in detail. Finally, Section 6 draws some conclusions.

2. THE SECURE TECHNOLOGY OF VPN

The transmitted information on the VPN network [7] is private, therefore VPN users should pay more attention to the security of data. The schematic diagram of VPN is shown in Fig. 1.

Four kinds of technologies are adopted to ensure the security, which are listed below: Tunneling, Encryption & Decryption, Key Management and Authentication.

1)Tunneling Technology

The core idea of this technology is to transmit data packages on the tunnel. The tunnel is formed by the tunnel protocol, which is divided into second and third layer tunnel protocols. The second layer tunnel protocol is to encapsulate diverse kinds of network protocols into PPP, and then load the entire data package into the tunnel protocol. The third-layer tunnel protocol is to load directly diverse kinds of network protocols into the tunnel protocol, and the formed data package is transmitted by the third-layer protocol. Common third-layer tunnel protocols include VTP and IP Security (IPSec), which is formed by a group of RFC documents. It defines a system to provide such services as secure protocol selection, secure algorithm and the key used by the algorithm, and provides secure measures on the IP layer.

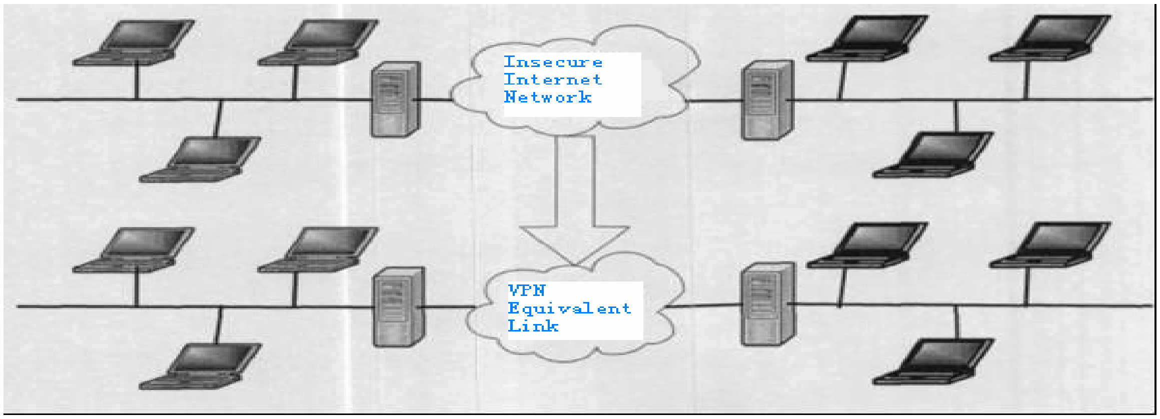


Fig. 1 The Schematic Diagram Of VPN

2)Encryption & Decryption Technology

This technology is more mature in data communication field and can be directly used by VPN, which is described in detail in the fourth part.

3)Key Management Technology

The main task of this technology is how to transmit the keys securely on the public network. The key adopted by this encryption algorithm [11] is not safe because it can be cracked by means of plaintext attack. The current key management includes SKIP and ISAKMP/OAKLEY. SKIP can take advantage of the calculus rules of Diffie-Hellman to transmit the key on the network, whereas ISAKMP can have two keys by both parties, that is, public key and private key.

4)Authentication Technology

This technology is used to prevent data from being forged and interpolated, which adopts a kind of new technology called digest. The digest technology is to map a long message into a short one which is called digest by the function transition, and it is nearly impossible to have the same digests for two different messages. Such characteristic is important to verify data integrity and identify user authentication. It is important to confirm the user identity before the tunnel connection, thus the system can further perform resource access control and user authorization[5].

3. THE CONSTRUCTION PROCEDURE OF SOFTWARE VPN SERVER BASED ON ISA SERVER

3.1 Traditional Hardware VPN Server Has The Following Disadvantages

- The traditional hardware VPN server has a capacity limitation, for example, many users purchased 30 concurrent VPN connection devices initially. If the demand for users exceeds 30, then the company will discard the original devices, and has to purchase new VPN devices of more capacity, thus the original investment will be wasted.

- The hardware VPN is simple to construct network, and has a fixed configuration. Generally speaking, the hardware VPN has a few interfaces, and fits for common enterprises. If a company has more complex and flexible requests for network, then the common hardware VPN is hard to meet these needs.

- The hardware VPN is weak in compatibility. The common hardware VPN has adopted its own standard or protocol, but not the industrial standard. When a company wants to construct VPN network, the problem of mutual connection and communication will occur unless all the devices are provided by the same manufacturer.

- The hardware VPN is hard to maintain. The common hardware VPN is tested and debugged by its own technicians. When the users want to customize the VPN network or make a small change after using a long time, they have no choice but to resort to the manufacturer’s technicians.

- The traditional hardware VPN is not fit for the network administrators to construct, and not for them to manage.

3.2 The Solution Of Software VPN Server

In this fast development times, the VPN server should be fully controlled by network administrators, or the constructed VPN network is easy for them to manage. With the development of increasing improvement of PC server hardware and the continued decline in costs, the software VPN Server has incomparable advantages from the diverse aspects of cost, performance, reliability and security [6].

(1)The protocol of software VPN server network

In the engineering practice, the computer acting as a VPN Server has a high performance, for example, its main frequency is above 4.0GHz, and has more than 4GB memory. Then Windows server 2003 and the ISA Server 2010 are installed on the server. This server is equipped with two network interface cards, one is connected to the core switch, while the other is directly connected to the Internet.

(2)The construction steps of software VPN Server

The main network components include VPN server, windows server 2003 and certificate server. Among them, the active directory is installed on the windows server 2003, at the same time both the certificate server and the VPN server can take advantage of the functions of active directory, whereas the VPN clients do not need to use the active directory. We make the following assumptions: The domain name and IP address of the active directory is separately set as slxxw.com and 192.168.3.1/24. Meanwhile the IP address of the certificate server is 192.168.3.2/24. The internal and external IP address of VPN server is set as 192.168.3.100/24 and 203.210.104.125/24 respectively. We must emphasize that the VPN server possesses two network adapters, but the certificate server and the active directory server has only one network adapter respectively.

The construction steps of software VPN Server is described in detail as follows:

- The windows server 2003 has been installed on the computer as an active directory server, and the IP address and the DNS name have been set as shown above.

- The IP address is set on the computer as a certificate server, and it is added to the active directory as a member server and capable to provide certificate service as needed. In practical application, the certificate server and the active directory server can be the same computer.

- We separately set the internal and external IP address and DNS server on the computer as VPN server, and attach active directory as a member server, then we install ISA Server 2010 to configure it to be a VPN server.

- We can create VPN users and user groups, and then create rules on the VPN server.

- We install certificate service on the Windows server 2003, and issue the certificate for the VPN server.

- Finally we configure the VPN clients, and make practical tests by using L2TP/IPSec.

3.3 The Advantages Of Software VPN Server

The constructed VPN server as mentioned above is better than the traditional hardware VPN solution from these aspects of performance, speed or security. Besides, it has the following especial advantages.

- It can protect users’ investment, and can fully perform the current hardware capacity. For the common hardware VPN server, its CPU can reach the level of P4 800MHz. But if we adopt the solution of software VPN server, then we can select the current prevailing hardware to achieve the bigger performance-to-price ratio.

- It can be customized flexibly. Generally speaking, the VPN server can connect two different networks, that is internal and external network. In our solution, we can make the VPN server connect to several different networks very conveniently. The only thing for us to do is to install different network cards on the VPN server and make different cards connect to different networks.

- In our solution, we adopt all the Microsoft products to achieve the maximal compatibility. For example, the server is configured windows server

2003 and ISA server 2010, whereas the clients are configured windows vista, windows xp and so on.

- It has a flexible expansion. As we know, the number of concurrent connections supported by a windows server 2003 is limited. If the number of concurrent connections exceeds the preset value in practical application, we can add a number of servers to achieve the aim of expanding the capacity, at the same time the original server can be used continuously.

4. Encryption-Decryption Algorithm

4.1 Aes Encryption Algorithm

The block and key length of Rijndael encryption algorithm can be specified independently for the 128-bit, 192-bit or 256-bit. Rijndael block cipher algorithm mainly includes the nonlinear components, linear elements and round key. All the operations of the algorithm are complete byte operations. The Rijndael algorithm uses round iterative structure during the encryption process and s-box, which is selected by the inverse operation of multiplication in the finite field GF (2^8) [1].

4.2 Ecc Encryption Algorithm

(1)The principle of ECC encryption algorithm

This cryptosystem uses finite point groups of elliptic curves over finite fields in place of finite cyclic groups based on the discrete logarithm problem. Compared with RSA cryptosystem, ECC cryptosystem has great security and technology advantages. The established elliptic curve cryptosystem has two potential advantages: one is that the inexhaustible elliptic curves can be used to construct the finite point group of the elliptic curves; second is that there is no calculation of sub-index algorithm of finite point group of the elliptic curve discrete logarithm problem. Therefore ECC is considered to be the most common public key cryptography of the next generation.

(2)domain parameters of elliptic curves

The order of the curve is defined as the number of all the points on elliptic curves, including infinity, which is difficult to precisely calculate its value, but we can calculate it according to Hasse theorem. As we know, the point finiteness on the elliptic curve groups and the uncertainty of the number of points are excellent properties for encryption, because these curves simply contain a number of discrete points, the attacker does not know how to apply the geometric relationships. The implementation of ECC is determined by the elliptic curve domain parameters, which include the base domain, curve equation of elliptic curves, curve base point, the order of the base point et al. Elliptic curve domain parameters are public and shared by two parties.

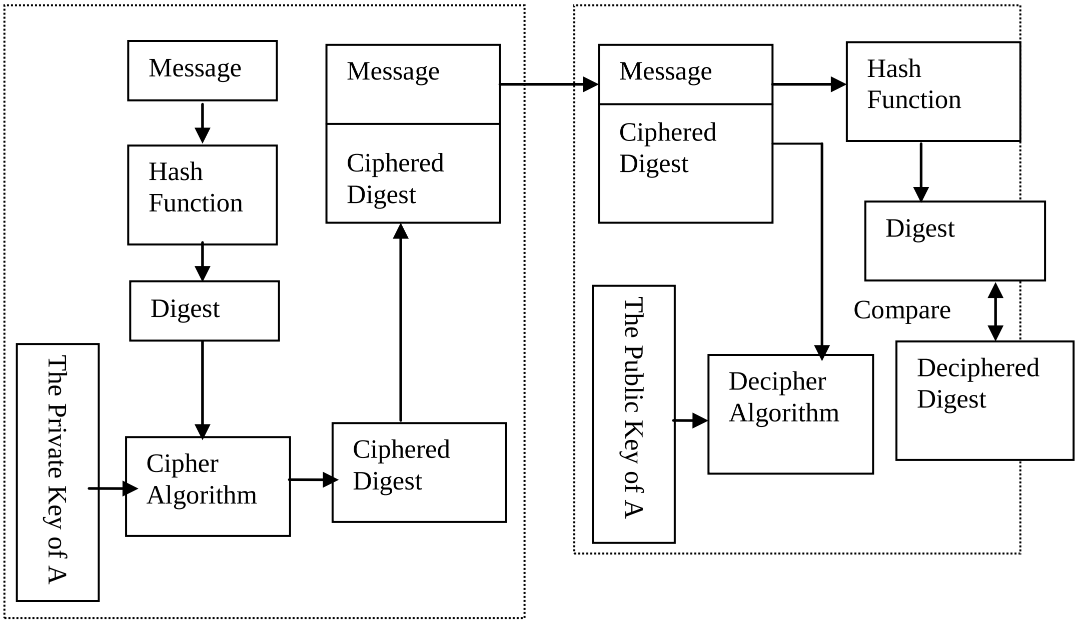


Fig.2 The Principle Of Digital Signature

(3)Elliptic curve discrete logarithm problem

Every asymmetric cryptosystem is based on the computational difficulty of a mathematical problem, furthermore, The security of ECC is based on the computational difficulty of the discrete logarithm problem on elliptic curves. The elliptic curve discrete logarithm problem (ECDLP) can be described as follows: For the elliptic curve E over a finite field, P and Q are two points on the curve E, and there exists nP=Q, then the mathematical puzzle of calculating positive integer n is just the elliptic curve discrete logarithm problem. It is well known that solving the discrete logarithm problem over finite domain is a recognized puzzle, while solving the elliptic curve discrete logarithm problem [4,10] is much harder than the former.

4.3 Digital Signature

Digital signature refers to the data obtained by the users to encrypt the Hash digest of original data with their own private key. The data receiver uses the sender's public key to decipher the digital signature attached on the original information to get Hash digest, and compares it with the Hash digest generated by the original data, thus he can be sure whether the original information is to be forged or not. This helps to ensure that the source of the authenticity and the integrity of data transmission. The principle of digital signature is shown in Fig.2.

4.4 The Introduction Of Openssl

SSL is the abbreviation of secure socket layer, which can provide secret transmission on the Internet. OpenSSL has realized the protocols of SSL/TLS (Transport Layer Security). Generally speaking, OpenSSL is divided into three parts, that is, SSL protocols, cipher algorithm library and application instructions. The structure chart of OpenSSL is shown in Fig. 3.

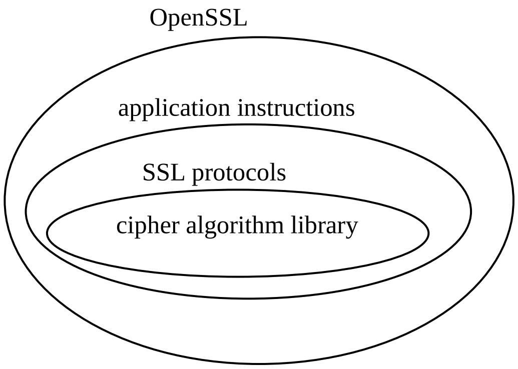


Fig.3 The Structure Chart Of Openssl

5. THE SECURE DATA TRANSMISSION ALGORITHM BASED ON VPN AND OPENSSL

In order to make full use of advantages of symmetric and asymmetric crypto-systems and overcome the shortcomings of key management and distribution to promote the application of cipher technology in information security transmission, we combine the advantages of two kinds of crypto-systems to put forward a kind of secure data transmission algorithm.

5.1 The Principle Of Secure Data Transmission Algorithm

The core idea of secure data transmission algorithm is described as follows: we encrypt the plaintext with the symmetric cipher algorithm, and then encrypt the key and digital signature belonged to the symmetric encryption algorithm with the public key algorithm. The sender encrypts the plaintext P with the key KAES belonged to the AES algorithm. To ensure the security of the cipher algorithm and simplification of key management, the sender uses the key KAES only once (that is, one at a time). The working process of the secure data transmission algorithm is listed as follows:

(1)The sender encrypts K_{AES} with the recipient ECC public key K_{pubb} to form C_k;

(2)The sender encrypts the signature information M with its own ECC private key K_{pria} to form C_M;

(3)The sender encrypts the plaintext P and the ciphertext C_M with K_{AES} and merges C_k to form the ciphertext C;

(4)The receiver deciphers C_k with its own ECC private key K_{prib} to obtain K_{AES};

(5)The receiver deciphers the ciphertext C with K_{AES} to obtain the plaintext P and the ciphered signature C_M;

(6)The receiver deciphers C_M with the sender's ECC public key K_{puba} to obtain the signature M.

At this point, the receiver obtains the original information P after signature verification.

5.2 The Advantages Of Secure Data Transmission Algorithm

It is not difficult for us to see that the secure data transmission algorithm has the following advantages:

- Due to AES key for data communication is encrypted and transmitted by ECC, so we do not need to send private secret key before communication;

- Confidential management of keys is like the same way of ECC, we only need to keep the confidential management of decryption key;

- The processing speed of encryption and decryption is largely the same way of AES, and that is, the time-consuming ECC processes only AES key. If the communication data are very long, the time of using ECC to process data is almost negligible;

- We send the keys with ECC, therefore we can also use it to perform digital signature.

5.3 The Performance Analysis of Secure Data Transmission Algorithm

For the Rijndael algorithm used by the senior encryption standard, the minimal group and key length also have 128 bits even if one computer can perform 256 times of key search per second, it will take at least 149 trillion years to complete AES key search, it is not feasible according to time and space. Therefore Rijndael algorithm is immune to strong attack for a long time from now on.

Algebraic computation attack is another attack against block ciphers. In this attack, the attacker will construct some polynomials by means of the pairs of input/output ciphers. If the element has a compact algebraic expression in the ciphers, and all the elements can be combined into an expression to control the complexity, then it is feasible for the algebraic attack to this cipher. Rijndael algorithm has simple and compact structure, so we can use an algebraic expression to describe the whole algorithm. The algebraic computation attack against Rijndael algorithm is equivalent to expand the algebraic expression, involving all the operations of s-boxes construction. We can learn from the complexity of s-boxes expression that it is not feasible for the attack to expand algebraic expression. Furthermore, if the attacker conducts direct access attack not by expansion, this method may be effective just from the judgment to determine the number of constants, but at the same time we should take into account the complexity of constructing linearly independent equations and solving it, so it may be under further research whether this attack method is valid.

We assume that one 1MIPS computer can perform 4x104 times of elliptic curve addition per second, this is an optimistic estimate. Therefore the number of one 1MIPS computer can perform elliptic curve addition is:

$$(4x10^4)x\ (60\ x\ 60\ x\ 24\ x365) \approx 2^{40}$$

Similarly, if 10,000 computers can perform parallel process, each hhas a speed of 1000MIPS per second, then the modulus length will reach $n \approx 2^{160}$, it will take 6,000 years to solve the ECDLP problem. A single calculation of elliptic curve discrete logarithm can only reveal one user's private key. Thus, under the existing conditions of solving methods and computing power, it is impossible to solve the ECDLP problem from the aspect of calculation quantity, so the security of ECC is ensured.

5.4 The Application of Secure Data Transmission Algorithm

There are many mountainous areas and abundant rainfall in Zhejiang province, and there are many reservoirs suitable for the construction of medium and small hydropower stations. Hydropower stations are located in mountainous areas with less convenient traffic in General. Here we cite the hydraulic information transmission between hydropower station departments as an example to illustrate the application of data transmission algorithm.

(1)The requirements of hydropower stations on the secure transmission of information are as follows.

- Important information is sent by the ciphertext, only legitimate recipients can decrypt the ciphertext to plaintext;

- The sender and the receiver can confirm each other's identity, and transmitted messages cannot be denied;

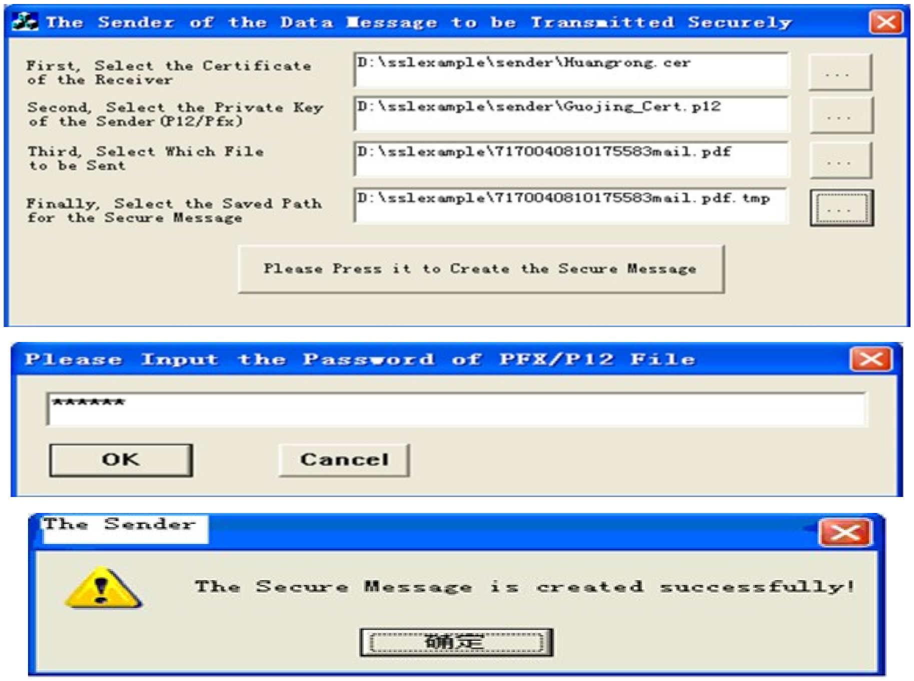
- If the illegal invader can access the network system, then any tampering and sabotage to the ciphertext by him can be found in time.

In the hydropower stations system, we can achieve the mutual information transmission between the VPN client and the server after the VPN and FTP servers have been set up by the data transmission algorithm.

(2)The application effectiveness

- The system creates barrier-free information exchange platform between the producer and receiver of information, ensuring the accuracy and real-time of information transmission, hence when the problem occurs between different departments, the phenomenon of shifting blame to each other has been significantly improved and enhanced.

- The system realizes the purpose of centralized control, finding a very good solution to lead uncontrollable problem. Plans and tasks assigned by the leaders can be monitored and understood in a timely manner, even the leaders are traveling. As long as they can have access to the internet, they can enter into their offices via the VPN client to understand the task states of different business units, and can process relevant problems in time.



The Sender of the Data Message to be Transmitted Securely

First, Select the Certificate of the Receiver: D:\sslexample\sender\Huangrong.cer

Second, Select the Private Key of the Sender(P12/Pfx): D:\sslexample\sender\Guojing_Cert.p12

Third, Select Which File to be Sent: D:\sslexample\7170040810175583mail.pdf

Finally, Select the Saved Path for the Secure Message: D:\sslexample\7170040810175583mail.pdf.tmp

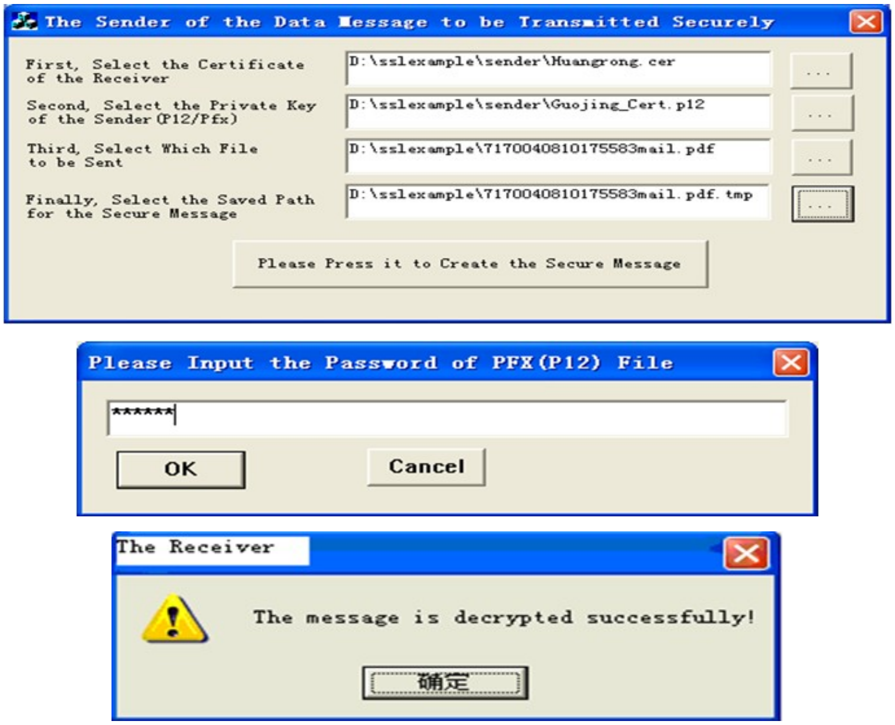
Please Input the Password of PFX/P12 File

******

The Sender

The Secure Message is created successfully!

Fig.4 The Running Results Of The Sender Program



The Sender of the Data Message to be Transmitted Securely

First, Select the Certificate of the Receiver: D:\sslexample\sender\Huangrong.cer

Second, Select the Private Key of the Sender(P12/Pfx): D:\sslexample\sender\Guojing_Cert.p12

Third, Select Which File to be Sent: D:\sslexample\7170040810175583mail.pdf

Finally, Select the Saved Path for the Secure Message: D:\sslexample\7170040810175583mail.pdf.tmp

Please Input the Password of PFX(P12) File

******

The Receiver

The message is decrypted successfully!

Fig. 5 The Running Results Of The Receiver Program

- Furthermore, we can establish a sharing platform on the basis of intranet access via VPN client, which can be a good platform for sharing information, knowledge and documents. Each employee can retrieve this sharing platform to obtain the information he needs. It is not only convenient for the employees, but also can gradually accumulate corporate knowledge resources.

For the important files of common formats, such as *.pdf, *.xlsx, *.docx, *.pptx files et al., we can use this algorithm to realize secure information transmission. Besides, we can also extend the application scope of this algorithm to other departments.

6. CONCLUSIONS

The secure data transmission algorithm combines characteristics of public key cryptography and symmetric cryptography. As is known to all, the former is easy to distribute keys and the latter is easy to calculate and provides a good and fast way for the secure information transmission. Engineering practice proves that this algorithm has many advantages, for example, it has simple principle and high security to some extent, and greatly meets the design criteria for the encryption algorithm. This algorithm can help us to achieve the goal of fast and securely transmitting information. The sender and receiver programs of this algorithm mainly implement the digital envelope and signature for the transmitted data files. The running results of the sender and receiver programs are shown as Fig.4 and Fig. 5.

ACKNOWLEDGMENTS

We would like to thank the research foundation of water conservancy department of Zhejiang province of China for contract RC0711, under which the present work was made possible.

REFERENCES

[1] Man Young Rhee, Internet Security: cryptographic principles, algorithms and protocols, Beijing: Tsinghua University Press, 2007.

[2] WANG Feng-ying, ”Dynamic Key 3DES Algorithm of Discrete System Based on Multi-dimension Chao”, Microelectronics & Computer, vol.22, pp.120-126, 2005.

[3] Falk A, “The IETF, the IRTF and the networking research community”, Computer Communication Review, v35, n5, pp. 69-70, 2005.

[4] ZHANG Yan, LIN Ying, HAO Lin, ”Summarize of Elliptic Curve Crypto-system Research”, Computer Engineering, vol.30, pp. 127-129, 2004.

[5] Gao guo xiang, Zhou yansong, “The Application of VPN Technology in the Shenyang Water Conservancy Information Network”, Northeast Water Conservancy and Hydropower, vol.44, pp 83-87,2008.

[6] Wang chun hai, The instances of VPN network Construction, Beijing: Science Press, 2008.

[7] Tao Guofang, Zhang Liang, “Layout of IPSec VPN with Cisco Router in a Frame-Relay Environment”, vol.22, pp.134-136, 2006.

[8] John Talbot, Dominic Welsh, Complexity and Cryptography An Introduction, New York:Cambridge University Press, 2006.

[9] Mandy Zandra Seet, Elliptic Curve Cryptography Improving the Pollard-Rho Algorithm[D], The University of New South Wales, 2007.

[10] S. M. Yen, Design and Computation of Public Key Crypto-systems[D], Ph.D. dissertation, National Cheng Hung University,1994.

[11] CHEDDAD A, CONDELL J, CURRAN K, et al. A Hash-based image encryption algorithm[J]. Opt. Comm., 2010, 283:879-893.

[12] TAO R, MENG X Y, WANG Y. Image encryption with multiorders of fractional Fourier transforms[J]. IEEE Transactions on Information forensics and Security, 2010, 5(4):734-738.

[13] ZHOU N R, DONG T J, WU J H. Novel image encryption algorithm based on multiple-parameter discrete fractional random transform[J]. Optics Communications, 2010, 283(11):3037-304