Research on the Application of Data Encryption Technology in Network Security Transmission

Junwei Li

College of Computer and Information Engineering, Xinxiang University, Xinxiang 453003, China

Abstract

With the development of information technology and popularization of the Internet, computer network security has gradually become the focus of attention. The data transmission on the network should ensure its confidentiality, authenticity, integrity and non-repudiation. The only effective way to solve these problems is to use modern cryptography. This paper makes full use of the fast speed of symmetric key cryptographic algorithm and the convenience in key management of public key cryptosystem. In this paper, the most advanced data encryption techniques, especially the AEC and ECC algorithms are proposed. The application program is in the Windows operating system, and a data encryption system technology program is designed. The system fully combines the symmetric key encryption algorithm and the public key encryption algorithm to provide a practical mode of operation for fast and secure transmission of confidential data. It also laid a practical and basic foundation for establishing a perfect and tight computer network security mechanism.

Keywords: Data Encryption, Network Security, Cryptography, Data transmission, Algorithm.

1. INTRODUCTION

With the rapid development of computer hardware technology and network communication technology, E-commerce, online banking, online shopping and other emerging things are emerging, which greatly enriches and facilitates people’s lives. However, at the same time, the network information leakage, tampering and counterfeiting, hacking, computer crime, computer virus spread, all these problems have become a major threat to network information security. Information security is increasingly becoming the focus of attention (Zhou et al., 2010; Li, 2011). At present, information security is an important part of national security. It has become a key problem affecting the country’s overall and long-term interests. So, the way to maintain network information security and ensure the safe transmission of information in the network is a very important part of network security. The core technology of information security and cryptography has been paid more and more attention.

In recent years, with the increasing concern about the security of network information, many network security technologies have appeared, and the password technology has also rapidly developed. The secret key is the key of the cryptography. And the cryptography can be divided into the symmetric key cryptosystem and the public key cryptosystem according to the different secret keys. Currently there are two encryption methods for data encryption (Stallings, 2003), one is the traditional private key encryption method, and the principle is using the encryption side with a key to encrypt the data and decrypt the side with the same key. From the ancient Roman times, this method has been used for the transmission of military intelligence. Modern cryptography improves its encryption process and is the standardized algorithm which is helpful to allow people to test the strength of encryption.

On the other side, the public key encryption method is completely different from the traditional encryption method. In this encryption scheme, encryption and decryption operations are performed using a pair of keys instead of a key, and a fair third party is theoretically required to hold one of the keys named public keys. This status generates a series of cryptographic problems, such as public key user acknowledgment, revocation of expired public keys and so on, which necessitates the creation of a certificate authority (CA) to perform these operations. We carefully analyze and master all kinds of existing encryption algorithms, and make full use of symmetric key cryptographic algorithm with fast encryption and decryption features and public key cryptography key management with the convenient features. Thus, a combination of encryption scheme is explored and designed, and the file encryption system is applied in the Windows operating system.
2. MATERIALS AND METHODS

2.1 Definition and Algorithm of Data Encryption

Data encryption technology refers to the use of cryptography and the relevant technology to replace or shift clear text information by the encryption key and encryption function. It becomes the worthless ciphertext, and is difficult to read by others. Information receiver can decrypt using the key and decrypt function to restore this ciphertext, and achieve the covert transmission of information. It is the core technology to protect the computer network data security. The information receiver can use the decryption key and decryption function to restore the ciphertext, and then realize the covert transmission of information, which is the core technology of computer network data security. Cryptography is one of the core technologies of information security.

At present, there are two encryption methods for data encryption. One of them is the traditional private key encryption method. The principle of this encryption method is very simple. The key encrypts the data, and the decryption party decrypts the data with the same key. From ancient Roman times, this method has been used for the transmission of military intelligence. The traditional data encryption methods have four algorithms. The first method is the replacement table algorithm. The replacement table algorithm is the simplest encryption algorithm, and each data segment corresponds to the displacement table in an offset. The corresponding offset value is encrypted file after the output. The decryption process then reads the information with reference to the substitution table. This method of encryption and decryption is simple and fast, but if the replacement table was obtained by others, encrypted files will be completely seen through. The second method is the improved replacement table algorithm. The algorithm is essentially the application of two or more replacement tables in a pseudo-random way, performing many times encryptions in order to increase the difficulty in ciphertext deciphering. The third is the cyclic shift and XOR operation algorithm. This algorithm is a transform data location algorithm that is a byte or word by changing the direction of a data stream in the cyclic shift, and then using the XOR operation to quickly encrypt the ciphertext (Zhu, 2012). The encryption algorithm can only operate on the computer, the ciphertext is also difficult to decipher. The last one is the cyclic redundancy check (CRC) algorithm, which is a 16-bit or 32-bit checksum hash function based on data, such as computer files or network data packets. A bit or two errors will inevitably lead to checksum error (Zhang, 2015). The encryption algorithm is good at verifying the errors caused by the transmission channel interference, and is widely used in file encryption transmission.

Modern cryptography solves this problem with a secret key, which consist of an algorithm, all possible plaintexts, ciphertexts (E) and keys. The transformed information is called plaintext, and the information after the transformation is called ciphertext. The conversion process from plaintext to ciphertext is called encryption. The transformation itself is a function of the encryption key K, denoted by Ek(P).

The ciphertext is transmitted through the communication channel to the destination. After that, it needs to revert to a meaningful plaintext, in order to be understood by the communication receiver. The conversion process that ciphertext C is reduced to a plain text P is called decryption or decryption. The transformation is to decrypt the key k as a function of the function, maked as Dk(C). The cryptographic decryption model is shown in Figure 1. Both of the encryption and decryption operations are using this key that means the operation depends on the key, so that encryption and decryption function now becomes:

\[ Ek(M) = C, \quad Dk(C) = M \]  

These functions have the following mathematical properties:

\[ Dk(Ek(M)) = M \]  

The security of all these algorithms is based on the security of the key rather than on the security of the details of the algorithm. This means that the algorithm can be made to the public and can be parsed to produce products. It does not matter even if the eavesdropper knows your algorithm. If he does not know the specific key you are using, it is impossible to read your message. In cryptography, the encryption and decryption algorithms are generally open to the attacker, as long as the decryption key is attained, they can decipher the ciphertext. So the key design is the core factor, and key protection has become the focus of the attack prevention. For key analysis, the key to the exhaustive guess attack is can not be avoided for any password system. However, when the key length is sufficiently random, the exhaustive guess should be practically impossible. For example, an encryption
algorithm with a key length of 256 bits and a key space of $2^{256}$ corresponds to 1077 orders of magnitude. If a computer can search 100 million times per second for a key space, the time required for an event in all searches will be greater than 1062 years. If the key space is small or the distribution has some predictability, then the attacker may use the relevant knowledge to narrow the search space, thus decipher the ciphertext (Liu, 2016; Song, 2014).

![Figure 1. A sketch of information encryption and decryption process and the location of the attacker](image)

2.2 Types and Characteristics of Data Encryption

Key-based algorithms usually have two types of symmetric algorithms and public-key algorithms. Symmetric encryption, also known as shared key encryption, refers to the sender and the receiver to use the same key. And in order to achieve the encryption and decryption of data, communication between the two sides agreed in the ciphertext. A public key is used for secure transmission. As a result, the security, confidentiality and integrity of the data transmission will not be affected, as long as the parties do not compromise the key. In the application of data encryption technology, symmetric encryption technology is the most common, and there are three data encryption algorithms, namely DES, AES and IDEA. DES data encryption standard algorithm which is mainly for binary data encryption, is a symmetric 64-bit data packet cipher. DES has the advantage of high encryption speed and encryption efficiency, and has a wide range of encryption. It has been widely and successful applied in the field of bank electronic funds transfer. Asymmetric encryption technology, also known as public key encryption, is using the combination of a pair of public key and private key.

The ciphertext encrypted with the public key can only be decrypted with the private key, whereas the ciphertext encrypted with the private key can only be decrypted with the public key. Difference in this application is that the key is divided into two kinds, that is, the public key and the private key. From the existing technology and equipment level, the key is not derived from the public key. Asymmetric encryption of data encryption algorithms are RSA, Diffie-Hellman, EIGamal, elliptic curve. A typical RSA algorithm can resist all currently known password attack, so it is the most widely used as well-known public key algorithm (Verma et al., 2011). In the symmetric encryption algorithm, only one key is used for both the sending and receiving sides to encrypt and decrypt the data, which requires the decryption party to know the encryption key beforehand. Symmetric encryption algorithm is characterized by open algorithm, and it has a lot of advantages, including the small amount of computation, encryption speed and high encryption efficiency. The downside is that both parties to the transaction have to use the same key, which means the security is not guaranteed.

In addition, every time a symmetric encryption algorithm is used for each pair of users, it is necessary to use a unique key that other people do not know. This will increase the number of keys owned by the sending and receiving parties, and the key management becomes a burden for users. Symmetric encryption algorithm is more difficult to use in distributed network systems, mainly because of key management difficulties, which is high cost. Asymmetric encryption technology is based on the application of key exchange protocol. The two sides of the communication before the exchange of keys, makes the key security risks can be eliminated for the confidentiality and provide data transmission with a strong guarantee. Symmetric encryption uses algorithms that are simpler than algorithms that use asymmetric encryption. Because these algorithms are simpler and the same key is used for both encryption and decryption of data, symmetric encryption is much faster than asymmetric encryption, especially when large amounts of data are encrypted. Therefore, public key algorithms are often used to encrypt a small number of key data, such as a traditional encryption algorithm, or digital signatures. In practical applications, usually symmetric encryption algorithm and asymmetric addition algorithm...
are used in combination, that is the use of symmetric encryption algorithm for large-capacity data encryption, and the use of symmetric encryption algorithm to pass symmetric encryption algorithm used by the key, through this method, the method can effectively increase the efficiency of the encryption and simplify the management of the key.

2.3 Computer network security transmission

With the development of computer network technology, network security has become the focus of computer network. Computer networks continue to reflect the unique advantages. At the same time, because of the openness of the network system, the sharing of resources, the complexity of the system, the diversity of the connection form, the inhomogeneity of the terminal distribution, the unknown ability of the network boundary, computer networks also bring a lot of problems. The most important issue is security. In a highly open computer network environment, unauthorized access, posing as legitimate users, destruction of data integrity, interference with the normal operation of the system, viruses and malicious attacks, wiretapping and other security problems have caused a great damage. China’s network security also exposed many problems. Although China has been rapid developed in the computer network technology, some infrastructure and network applications are also mostly relying on foreign technology and products. And people’s overall awareness of the computer network security is still lack. There are still many problems in the stability of the computer network and scalable areas. The system design does not meet the standard standards, thus serious impact was caused to the computer network security. Besides, there is the threat from some viruses which is destructive and contagious, and using the computer's instructions and program code for self-replication. The other way is passing the virus through spam to obtain user information. In addition, the network hardware configuration is not coordinated. Network hardware is the network hub, the entire network has a key role in the operation. Finally, the improper selection of network card will also cause the instability of the network system, while the security strategy and access configuration strategy and the complexity of the management system are also important issues. Internationally, especially the United States, Britain and other western developed countries began a high degree of concern about network and information security issues in the mid-1970s. After 30 years of development, many practical results have been made in the theoretical research, product development, standard-setting, security system construction, security awareness education and personnel training and so on. The content of computer network security contains a wide range of rules and practices to build computer networks so that information is not compromised. Transmission security is to take measures to protect the transmission is not intercepted and used by other means except cryptography. In addition to transport security, computer network security also includes confidentiality security, radiation safety and physical security.

![Figure 2. The communication security layer diagram](image)

It is easy to see from figure 4 that the technical definition of security has a direct relationship with encryption and other technologies. As the security risk increases, the value of the system and the cost of security control increase. It is very useful for an organization to correctly assess risks that involve security or lack of security. In addition, the size of the network may eliminate security issues and may also increase the security issues.

Nowadays, the network security technology mainly includes virus prevention technology, firewall technology, intrusion detection technology, access control technology, vulnerability scanning technology, network protocol
security verification technology, data encryption technology and digital signature technology. Especially, the data encryption technology and digital signature technology belong to the category of cryptography (Xiang and Department, 2014). The most famous solution applied to the Internet is sockets layer (SSL), secure electronic transaction protocol (SET), virtual private Network (VPN), security authentication center and security smart card technology, which are all based on public key infrastructure (PKI)[H]. It can be seen that the password technology occupies a large proportion of information security in computer network information security technology.

2.4 The algorithm used in the data encryption system

2.4.1 The RSA algorithms

Commonly used public key algorithms are RSA algorithms, proposed by Rivest Shamir and Adleman and named with their initials (Ramesh and Suruliandi, 2013). RSA can implement encryption and digital signature functions using two keys. One is for the public key and the other is for the private key. With one key for the encryption, and you can use another key for decryption. The key length varies from 40 to 2048 bits, and encryption can also be divided into blocks of the plaintext. The block size is variable, but can not exceed the length of the key.

The algorithm converted each block of the plaintext into the same key length ciphertext block. If the key is longer, the encryption effect is better. But the cost of encryption and decryption is large, so a compromise between security and performance considerations, the general 64-bit is more appropriate. One of the more well-known RSA applications is SSL. The advantage of a public key is that a secure communication can be carried out, as long as the server side believes that the requesting entity certificate authority CA is reliable. The server side of their own resources can be based on the reliability of the customer CA issuing authority. To implement the RSA algorithm, firstly a private key is generated following the process: (1) two prime p and q whose length is K/2 is randomly generated; (2) the equation publicKey=p*q is calculated; (3) an encryption key (E) is randomly generated, and need to meet the requirements:

\[ 2 \leq \text{keyE} \leq \Phi(n) - 1 \tag{3} \]
\[ \Phi(n) = (P-1) \times (Q-1) \tag{4} \]

Equation (3) is the necessary and sufficient condition for solution of the decryption key in equation (5),

\[ \text{keyE} \times \text{keyD} \mod \Phi(n) = 1 \tag{5} \]

The decryption key is solved. Secondly, plaintext is encrypted and the ciphertext is decrypted, the mathematical process was shown in the following equations:

\[ c = m^{\text{keyE}} \mod \text{publicKey} \tag{6} \]
\[ m = c^{\text{keyE}} \mod \text{publicKey} \tag{7} \]

Where the m is plaintext and the c is ciphertext.

2.4.2 The ECC algorithm

Another common algorithm is elliptic curve cryptosystem (ECC) proposed by Neil Koblitz and Victor Miller (Tamikodi and Rama, 2015). ECC is a new cryptographic algorithm. The security of ECC is composed of elliptic curve discrete logarithm problem (ECDLP). This is an NP-complete problem. Elliptic curve cryptosystem is a cryptosystem applied to public key cryptosystem. Compared with RSA cryptosystem, there are many advantages, and based on the difficulty of EDLP, it is quite easy to construct public key cryptosystem and digital signature algorithm. Because the elliptic curve on the first group of operations can eventually be reduced to its background on the domain of not more than 15 times the multiplication, and thus it’s easy to
implement (Xiang and Department, 2014). The elliptic curve cryptosystem is based on a finite elliptic curve finite group \( \text{E}(\text{GF}(p)) \). However, in the concrete implementation, the cryptosystem needn’t be chosen for every time, which is too time-consuming. And usually the approach is to create a sufficient number of secure elliptic curve libraries, and then define a system parameter that allows the cryptosystem to be performed under different system parameters. Figure 3 shows the process of encryption and decryption of ECC. The elliptic curve encryption mechanism is as follows, with the domain parameters \( R = (q, a, b, G, n, h) \), the receiver B’s public-private key pair is \( (k, k) \), and the sender A has a copy of k. A sends the message m to B:

1. A random number \( r \) is generated on the set of \([1, n-1]\);
2. The ciphertext \( c_1 = m + rKc_2 \) is calculated;
3. \((c_1, c_2)\) is transferred to B;

the ciphertext \((c_1, c_2)\) is decrypted and B is executed:

the following equation is solved:

\[
c_1 - Kc_2 = m + rK - K(rG)
\]  

(8)

In this process, if there is an intruder, he can only see \( K, G, c_1, c_2, \) and \( k \) is attained by \( K, G \) or \( c_3 \). The parameters \( G \) and \( r \) are relatively difficult to obtain, so he cannot transfer the plaintext information between A and B.

To decipher this cryptographic scheme, the attacker needs to compute \( k \) according to the given \( G \) and \( kG \), which are considered difficult. It’s notable that a private key is a pair of numeric values. If this key is to be used as a conventionally encrypted session key, a single value must be generated. Compared with the RSA system, the elliptic curve cryptosystem has the advantages of higher security, less computation, faster processing speed, less storage space, and lower bandwidth requirement. Table 1 compared its security.

![Figure 3. The process of encryption and decryption of ECC](image)

**Table 1** Comparison of Elliptic Curve Cryptosystem and RSA Cryptosystem Security

<table>
<thead>
<tr>
<th>Key length of ECC</th>
<th>Key length of RSA</th>
<th>Computer decryption time (years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>160</td>
<td>1024</td>
<td>1E+12</td>
</tr>
<tr>
<td>320</td>
<td>5120</td>
<td>1E+36</td>
</tr>
<tr>
<td>600</td>
<td>21000</td>
<td>1E+68</td>
</tr>
<tr>
<td>1200</td>
<td>120000</td>
<td>1E+168</td>
</tr>
</tbody>
</table>

In addition, data encryption standard(DES) is an encryption algorithm designed by IBM. In 1976, it was chosen as a standard algorithm. A key size of 64 bits was used in the algorithm and blocks of 64 bits are encrypted. The key size is 64 bits are used in the algorithm to encrypt the data instead of 56 bits. The other 8 bits are used for parity checking. Figure 4 shows a key schedule of the DES.
3.RESULTS AND DISCUSSION

3.1 The Design of File Encryption System

The public-key scheme is slower than the symmetric-key scheme. Therefore, it is common to combine the open key and the symmetric key technique to achieve the best performance. That is, the symmetric key is transmitted between the communicating parties by the open key technique. Symmetric key is the actual transmission of data encryption. Considering the advantages and disadvantages of symmetric key cryptography and public key cryptography, as well as the threat posed by the development of cryptanalysis techniques in recent years, this file encryption system applies to the international standardization organization, and developed the layered architecture of an open system interconnection reference model for the computer network, that is the ISO reference model which is applied on the top layer.

The application mode in the network is end-to-end encryption. The so-called end-to-end encryption means that the source host or the front-end of the top layer which is from the transmission layer to the application layer on the encryption of the data transmission. And the transmission network in a ciphertext to the host was decrypted to original note. That is, data encryption and decryption are only at the two ends of the file transmission and the data in the entire transmission process are in the form of dense state. The advantage of this end-to-end network encryption approach is that it provides true end-user security to the end user, no matter where the data transmission path is. Even the routers cannot see plaintext or impersonate the sender. For a large amount of data in the network transmission, we use the password length symmetric encryption algorithm for encryption, while the symmetric cryptographic algorithm is encrypted using the crypto-length elliptic curve public key encryption algorithm. This method not only ensures the security of data and improves the speed of data encryption and decryption, but also realizes the requirement of data information security and fast transmission.

File encryption system server uses multi-threading technology to ensure that each user can simultaneously decrypt the file. The system is divided into three related program modules, namely, the server-side management applications, server-side communications applications and client applications, to improve its efficiency. The overall system architecture is shown in Figure 5. The management application, the communication application module and the client module are at the top level of the system and they have responsibility for receiving the user instructions, displaying feedback information, and calling the lower module during the data processing. Especially, the lower module of the management application comprises five modules, including a key management module, an encryption packing module, a user data management module, a file information management module, a user changing password and a receiving public key module. The lower module of the communication application includes three modules: module, authentication module and file password sending module. However, the lower module of client application comprises four modules: change password module, key transmission module, file decryption module and communication module.
3.2 The results of the file encryption system

The management server application has the functions of key management, packing encrypted files, user database management, file database management, accepting user changing password information and receiving user public key. The algorithm choosing main interface was shown in Figure 6. From the main interface, we can see all the available algorithms for the file encryption system. The key field is to write a desired key to introduce on the algorithm and the box under the key field is to write down the text to encrypt or decrypt.

User data management is to add, modify, query, delete user information, including user passwords, user rights, user phone, user units and so on. User data management and file information management using Acess 2000 database management system, using the same database. The user data management uses the pUser table in the database, which has the following fields: UserID, UserName, UserAble, UserPhone and UserDep. Figure 7 shows the function of deciphering time with key length of ECC, RSA&ECC and RSA respectively.

In summary, the file encryption system implementation process is mainly the following two aspects. The first is the server-side application:
Register the ODBC data source. The data source name is service, type Microsoft Access, the user name is Admin, the password is pass, and the database file name is server database.mdb.

The keys of server (server.pk) are generated in the ECC module.

Modular user data management module increases the system user information.

Encryption module is packed to select the file and the original encrypted file named.en is generated, the original ID number of the part and the encrypted password are written in the file information database.

The communications server application and the network communication service are started.

And then the second step is the client application:

(1) The server’s public key server.pk is accessed, and added to the client application suction sub-directory named “/KEY/”, the user's own public key and private key file are generated, the file name is “the user name.sk” or “user name.pk”.

(2) The server’s address, the use’s name and password are set.

(3) The user’s own password is modified.

(4) The user’s public key is sent to the server.

(5) The file to decrypt is selected.

(6) The file began to decrypt, and the message box shows the decryption process information tips. If there are multiple files to decrypt, the steps will be repeated.

File encryption system of the three applications, including service.exe, serviceSer.exe and client are developed and compiled in the Windows XP SP2+Visual C++6.0 environment. The function of each module in the three operating systems installed on the computer LAN running through the Windows XP SP2 system.

4. CONCLUSION

This paper mainly describes the design and implementation process of the file encryption system application. In order to the transmission of data, encryption system design should consider the following requirements: to meet the communication data encryption purposes, and to verify the integrity of the data received. Thus we can ensure the authenticity of the data and prevent the two sides of the transmission data from the denial. For the seek of ensuring the authenticity, integrity and reliability of information, this paper comprehensively integrates the advantages of various algorithms, and combines the symmetric key algorithm and the public key algorithm to avoid the use of one algorithm alone. At the same time, the use of database technology on the user permissions in hierarchical management makes different users have different reading rights. Because the encryption system makes full use of the characteristics of fast decryption in symmetric key cryptography algorithm and management feature in the public key cryptography, besides, the digital signature algorithm is also combined to guarantee the security and integrity of the information, it is easy to implement and full of high security. Security in the field of network transmission has broad application prospects.

REFERENCES


