Analysis of Electronic Mail Encryption Technology

He Junhui
（Zhengzhou Information Science and Technology Institute，Zhengzhou 450001，China）
hjhkong@qq.com

Abstract: With the development of the Internet,e-mail becomes one of the most widely used services on the Internet with its low price and convenient operation.However,with the development of e-mail,the value of the message is increasing,and the security issues have become increasingly prominent,so the e-mail encryption is particularly important.

Key words: E-mail；information leak；encryption method

Introduction

The existence of rogue program, virus, Trojan horse and other unsafe factors enable the e-mail to face being deceived or attacked, or a series of security risks in the process of use. Many enterprises and individuals are worried that the e-mail would become the new channel of divulging a secret, make the secret restricted data be stolen by other people, lead the enterprises or individuals to be shamed, and even lead to a tremendous economic loss. Some e-mails are even involved with the national secret information, and the consequence is dreadful once a secret is divulged. These anxieties are not the rumors. Such as the business contracts, the patented technologies, the market strategy are the confidential data that are related to the enterprises' survival and development, and there are countless cases with the heavy losses that are caused by the disclosure of e-mail. Using individual e-mail to process massive official business, the American incumbent Secretary of State Hillary still get into the trouble of the e-mail issue, and there are much secret information in these e-mails. Thus it can be seen, e-mail has become the principal channel that the units and enterprises divulge a secret at the present stage, so its safety protection is imperative. As the e-mail rapidly grows, people have increasingly attached the great importance to its effective safety protection. The key to protecting the e-mail is enciphering it with the cryptographic technique, and it only permits the appointed validated users to read e-mail through this method, which can guarantee the security of the information transmission.

1. Research background

The security threats that the e-mail faces mainly have the following forms:

(1) If the e-mail does not have any encryption processing in the entire process of transmission, the attacker can easily steal the users' important information from the e-mail in the process of this public transmission;

(2) In the public network, the attacker can send e-mails by the illegal use of users' e-mail addresses, and this process can be completed through changing some settings of the computer in the situation that the users know nothing;

Copyright © 2017, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

(3) If the users send the e-mail to the strange user by mistake, and the e-mail doesn't have any encryption processing, the strange receiver can easily read the e-mail content and even use this e-mail to do the illegal online activity;

(4) The sender denies a truth,that is,he does not acknowledge that he has sent an e-mail to the receiver.

2. The e-mail encryption technology

2.1 The symmetric encryption technology

The symmetric encryption algorithm uses the same key in both encryption and decryption, and requests both sides to have the same key before the correspondence. In this algorithm, the sender does not have to possess the ability of decoding while sending the message, but only needs to encipher the plaintext, turns it into the ciphertext that the third party is unable to obtain any information, and then sends it to the receiver. If the receiver wants to obtain the raw data, he must decrypt the ciphertext with the decryption key that both sides obtain before the correspondence[1]. This algorithm is a cipher algorithm with a mature technique, but it also has the serious shortcomings:

(1)Both sides of the correspondence use the same key, and any third party can decode the message easily if the key is divulged.

(2)Under this encryption system, both sides of the correspondence are requested to use the only key that any third party would not know. Therefore, in the large-scale correspondence network, the key distribution before the correspondence has become a prominent question.

2.2 The encryption technology of traditional asymmetric cryptographic system (PKI/CA)

PKI refers to the public key infrastructure. It can provide the unique verification of user's identification through the confidentiality of user's private key in the public key cryptosystem[2]. CA refers to the certificate authority, and also called the certification center. It solves many kinds of problems about the network trust in many aspects. PKI/CA is mainly composed of three parts: the user, the registration authority, and the certificate agency. Its working principles are shown in Figure 1.

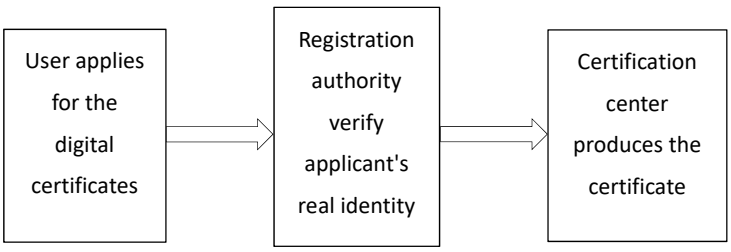

Figure 1: The working principle of PKI/CA

As is shown in the figure, the registration authority acts as the middle entity between user and CA, and its

major function is to examine the applicant's identity in the registration of certificate. After getting this verification, the user's information will be uploaded to CA, and then the certificate will be made. In addition, the registration authority will also submit the update, the cancellation and other duties of a certificate to CA[3]. The certification center will distribute the digital certificates to all the users in this trust system, which can conform that the user'identity has been already got the verification. It can be seen that CA is regarded as the trusted third party in this system. Therefore, in the correspondence, the method that can facilitate determining whether the users on both sides are the users in this trust system or not is that examining both sides' digital certificates.

The PKI/CA can conduct the encryption and decryption, the signature and verification on the data transmitting on the network, can guarantee that the e-mail would not be changed in the transmission process, and the senders cannot deny the message which they had sent. Except for the receiver and sender, the third party is unable to obtain the e-mail, and the sender can confirm the receiver's identity through the verification of the digital certificates.

At present, this encryption technology becomes quite mature after the development, but there are still some shortcomings while applied into the e-mail encryption, for example:

(1)The key management is not convenient.

(2)The key`s exchange are the premise of both the encryption and decryption of the PKI/CA, so the complexity is the characteristic of this process.

(3)It is quite complicated to obtain the CA certificate, so there is a certain difficulty in the popularization of this e-mail encryption technology.

As can be seen, PKI/CA is only suitable for some high-end electronic commerce and high-end users.

2.3 Chain encryption technology

The chain encryption cryptosystem is a kind of the ingenious e-mail encryption technology that integrates the symmetric encryption algorithm and the asymmetric encryption algorithm.Its working mode is shown in Figure 2. In the chain encryption cryptosystem, Sender A will choose a session key in the encryption, conduct the first encryption to the plaintext with a symmetric encryption algorithm, and then conduct the second encryption on the ciphertext that is obtained from the first encryption with the asymmetric cryptographic algorithm RSA. When decoding, Receiver B firstly decrypts this session key with the RSA algorithm, then decrypts again after the corresponding symmetric algorithm, so as to obtain the plaintext.

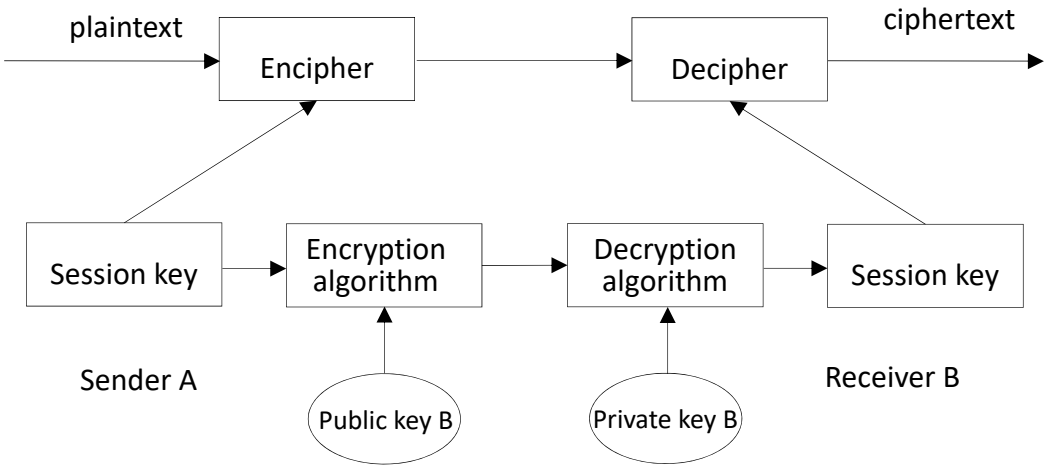

Figure 2:The working principle of the chain encryption technology

The chain encryption technology not only has the strong secrecy by the RSA algorithm, but also retains the rapidity of the symmetric encryption algorithm. In addition, the exchange of public key is based on the trusted mechanism, so the e-mail of the users who manage their own keys by themselves is safe. At present, the e-mail encryption software that uses the chain encryption cryptosystem is PGP(Pretty Good Privacy)[4].

2.4 The identity-based encryption technology

In 1984, Adi Shamir (the famous Israeli scientist, one of the inventors of the RSA system) proposed the identity-based cryptosystem idea, which greatly simplified the problem of key management in the traditional public key cryptosystem[5]. The Identity-Based Encryption (IBE) directly takes the character string that represents the user's identity as the public key, and is a new type of public key encryption system that doesn't directly obtain the public key from the public key certificate. Its working principle can be embodied through the correspondence of both sides: The public key is generated through the use of identity information that Sender A discloses, the trusted center produces the private key and pass it to Receiver B after confirming Sender A's identity, and finally Receiver B uses this private key to decrypt.

The work flows of the identity-based encryption are shown in Figure 3.

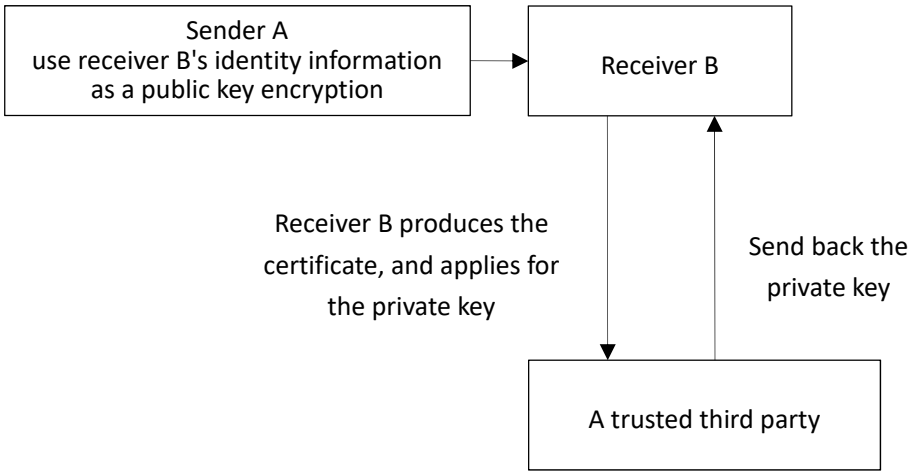

Figure 3: The working principles of the identity-based encryption technology

The IBE has become the hot spot in cryptology research after being proposed because of the simplification of the management of the public key. As one kind of new public-key cryptography mechanism, the IBE is regarded as an important effective method that can construct the public key trust system in the future. The Saiman E-mail Angel System is the typical product that uses this kind of cryptographic technique at present[6]. It is noteworthy that the server security in this system is important because the keys of all users are saved in the server end.

3. The comparison of four kinds of e-mail encryption technology

As the Internet and information technology grow, the e-mail encryption technology has increasingly become mature. Meanwhile, four kinds of typical encryption technologies that are analyzed in the paper have their own strong points. Based on the characteristics of the above four encryption technologies, we can obtain the comparison of the good and weak points that are shown in Table 1. In the practical application, we should select the appropriate encryption technology in view of their respective characteristics.

Table 1: The comparison table of the e-mail encryption technology

The commonly-used e-mail encryption technology	Advantages	Disadvantages
The symmetric encryption technology	The algorithm is public, the computation load is small, the encryption speed is fast, and the encryption efficiency is high	Use the same key, the security is low, and is easy to divulge
(PKI/CA) encryption technology	Guarantee the authenticity and Non-repudiation	The key management is complex, and it is difficult to obtain the CA certificate
Chain encryption technology	High speed and high-level security	The cost of maintenance and cancellation for the certificate is high
The status-based password encryption technology	It does not need any certificate, and the receiver's public key stems from his identity information The key has the service life, so it does not need to be abolished It can resist the attack of junk e-mail	It needs a centralized server, which increases the security risk of divulging

4. Conclusion

The present e-mail system is still facing the austere situation of divulging secrets, so the research regarding the e-mail encryption technology needs to be discussed unceasingly. Through the research and analysis of above four kinds of e-mail encryption technologies, it can be seen that commonly-used four kinds of encryption technologies have their own strong points. As the developers, they should choose the most appropriate encryption technology, and give dual attention to the security guarantees and encryption speed of the e-mail so as to guarantee that the users have the absolutely safe rights of privacy in the virtual network world.

References:

[1] 金晨辉,郑浩然,张少武,等.密码学[M].第一版.北京:高等教育出版社,2009.
[2] 罗萱.PKI 技术的基本原理及常规应用[J].电脑知识与技术.2014(24):5572-5573.
[3] 徐志大,南相浩.认证中心 CA 理论与开发技术[J].计算机工程与应用.2000(09):87-90.
[4] 丁丽,孙高峰.基于 PGP 的安全电子邮件应用研究[J].鄂州大学学报.2013(06):76-77.
[5] Shamir A.Identity-based cryptosystems and signature schemes[C]// Advances in cryptology-crypto`84.[s.l.]:Springer-Verlag,1984:47-51.
[6] 曾兵,杨宇,曹云飞.基于身份加密(IBE)技术研究[J].信息安全与通信保密.2011(04):64-66.