ATLANTIS PRESS
Advances in Computer Science Research, volume 59
7th International Conference on Education, Management, Computer and Medicine (EMCM 2016)

Analysis of Data Encryption Technology and Secure Electronic Transaction

Jian Wang
[1]Jiangxi Vocational College of Mechanical&Electrical Technology;
[2]Wuhan University of Technology

Keywords: Data; Encryption technology; Secure electronic; Transaction

Abstract. With the rapid development of the modern Internet, e-commerce has been greatly promoted. The advantages of e-commerce gradually appear, as a result, virtual enterprise, virtual bank, Internet marketing, online shopping, online payment, online advertising business and a large number of new business which have never been heard of before are familiar to and identified by people. These new business also reflect from the other side that the e-commerce is influencing the society and economy. E-commerce is changing people's life and the development process of the whole society. At the same time, the problems of network security have become the most important issue of e-commerce, in which confidentiality, integrity and non repudiation become the key to the security of e-commerce. To achieve complete e-commerce, many aspects should be considered. In addition to buyers and sellers, the banks or financial institutions, government agencies, certification bodies, distribution centers and other institutions should also be involved in e-commerce activities. Since the parties involved in e-commerce do not meet each other in physical place, so the whole process of e-commerce is not like the business activity in the physical world. Online banking, online payment and other conditions, as well as data encryption, digital signature and other technologies play an important role in e-commerce.

Introduction

With the development of the Internet technology, e-commerce has gradually become a new business mode for people. But due to the openness of the Internet and other factors, the security problem of e-commerce has been one of the important reasons that block the further development of e-commerce. The security problems of e-commerce mainly include the interrupt and paralysis of the system, information stealing, information tampering, information counterfeit, repudiation of transaction behaviors and other aspects, which can be divided into bottom physical system security and upper business logic system security from the perspective of logic. The bottom physical system security mainly refers to the security of the computer network system that supports the operation of the e-commerce system. The upper business logic system security mainly refers to the security of the e-commerce transaction which ensures the smooth development of e-commerce activities on the Internet. E-commerce transaction security problem refers to the information security of e-commerce transaction process. The security requirements contain confidentiality, integrity and non repudiation of information, as well as the certainty of the transaction identity. To ensure the security of electronic information security has become a hot issue in the present study. Encryption technology is an important technology of data security in e-commerce, which plays a very important foundation role to ensure confidentiality, reliability and review ability of business data communication.

Unsafe Factors in E-Commerce Transaction

When the traditional business models are used in the Internet, many security problems appear. The openness of the Internet brings many risks for online transaction, therefore, there are several security requirements as follows: first, the confidentiality of information; second, the certainty of the transaction identity; third, the non repudiation of information; fourth, non repairable. In the e-commerce transaction process on the Internet, transaction security is the core and key problem. Generally speaking, there are the following security risks in business security:

Stealing Information. If encryption is not used, when data information is delivered on the Internet in clear text, intruders can intercept the information at the gateway or router when the packet data passes. By repeatedly stealing and analysis, the rules and formats of the information can be found and the contents of the information can be obtained which causes the leakage of the transmission of information.

Tampering Information. In the process of transmission, the electronic transaction information may be modified, deleted or reproduced illegally by others, which makes the information lose authenticity and integrity.

Counterfeit. By mastering data format and tampering information, the attacker can counterfeit legitimate users to send counterfeit information or take the initiative to obtain information, and the remote user is difficult to distinguish. In addition, the third party is likely to counterfeit the identity of the transaction party to destroy the transaction or destroy the credit of the party which is counterfeited or steal the transaction results of the party which is counterfeited.

Malicious Damage. The computer network is vulnerable to the destruction of some malicious programs, which causes the destruction of e-commerce information, since the attacker can assess the network and modify the information in the network or hide in the network which is more serious.

Data Encryption Technology and Its Algorithm

There are two methods to design a high density cryptographic algorithm, in which one is to study all the possible solutions for all code analysis, and then to design a set of rules to defeat any one algorithm of these solutions and to construct an algorithm which can resist these solutions; the other one is to construct some algorithms. It is needed to solve some problems before decrypting these algorithms and these problems are considered unsolvable. This paper will introduce DES algorithm which belongs to the first one, while RSA belongs to the second.

According to whether the encryption key is public or not, encryption technology can be divided into two kinds of systems. The first is a symmetric encryption key system whose encryption key and decryption key are the same. For security, the key should be regularly changed. Symmetric algorithm is fast, so it is widely used when dealing with large amounts of data. The focus is to ensure the security of the key. Typical algorithms are DES and all kinds of deformations (such as Triple DES), IDEA, RC4, RC5 and the classical passwords (such as substitution passwords and cipher passwords), etc. Among these symmetric passwords, the most important is DES passwords. The second is the public key system and there is a public key which is public and a private key which is private. The public key and the private key have one-to-one relationship. The data encrypted with the public key can only be unlocked by the private key. The efficiency is lower than that of the symmetric encryption key system. The typical algorithms are RSA, knapsack passwords, Elliptic Curve, ElGamal algorithms and so on. The most representative and the most influential algorithms of the two systems which are DES and RSA are selected.

RSA Algorithm. RSA uses two encryption keys, one is the public key (the following is expressed as PK), one is the private key (the following is expressed as SK). The text is divided into blocks during encryption. The size of blocks is variable, but not more than the length of the encryption key. RSA turns the text into ciphertext with the same size of encryption keys. In general, the higher the security level is, the larger the key will be selected. The lower level of security is, the smaller the number will be selected. RSA security depends on the decomposition of large numbers, but it should be noted that whether it is equivalent to the decomposition of large numbers has not been proved theoretically. There is no proof that to decrypt the RSA must have a large number of decomposition.

DES. DES encryption uses the traditional method of transposition and replacement. In control of 56 bits key, 64 bit plaintext block is transformed into 64 bit ciphertext block. The encryption process includes 16-round encryption iterative and product cipher mode is used in each round.

In application, DES and RSA are generally combined with each other. DES has high encryption efficiency. The problem of encryption key storage should be solved, since the encryption key is easy to be leaked in transmission.

Application of Encryption Technology in E-Commerce

Digital Envelope. Digital envelope is a typical application of symmetric key encryption technology and asymmetric key encryption technology to ensure the confidentiality of information in e-commerce transactions. The application principle is the information sender encrypts the information by symmetric encryption key, and encrypts the symmetric encryption key by the public encryption key of the receiver (which is called the digital envelop). Then the symmetric encryption key and the encryption information should be sent to the receiver. The receiver opens the digital envelope with the corresponding private encryption key to get the symmetric encryption key, and then uses the symmetric encryption key to decrypt the information. The principle of applying digital envelope for information transmission is as shown in Fig. 1.

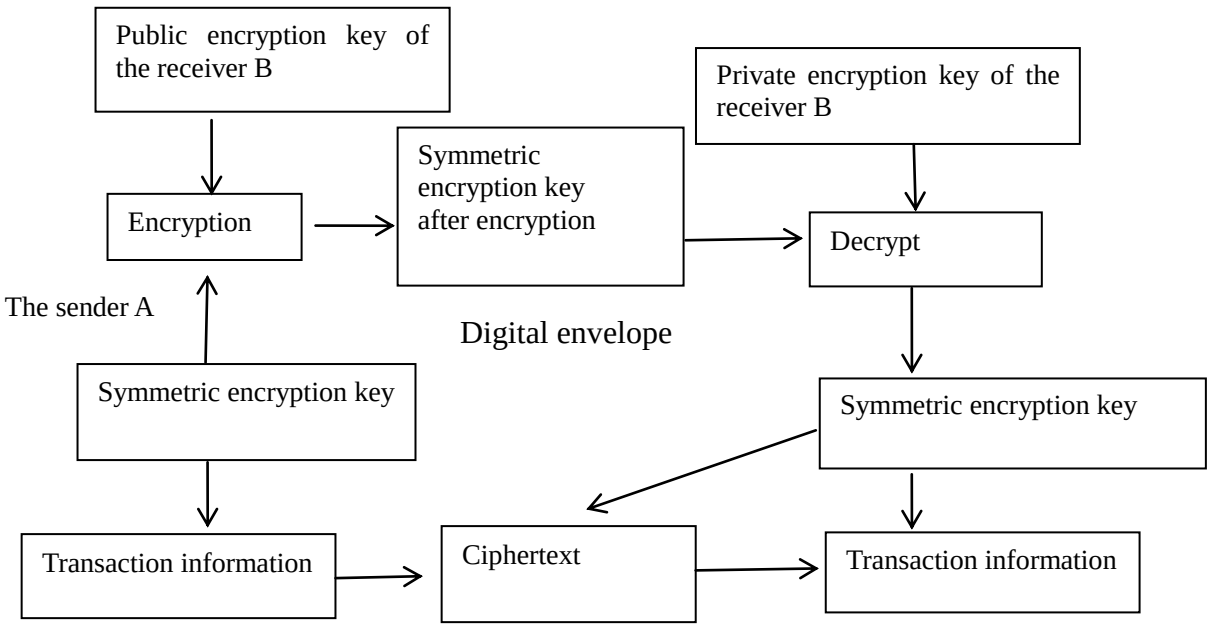

Figure 1. Applying digital envelope for information transmission

Digital envelope does not only have the flexibility of the public encryption key but also the high efficiency of the symmetric encryption key. In the process of e-commerce transactions, a number of important short information, such as bank accounts, passwords, etc. can be transmitted in a digital envelope.

Digital Summary and Digital Signature. The digital summary is to get the information string with fixed length to the information according to some mathematical algorithm (such as hash algorithm). The information string and the original information are correspondence, which means the digital summary produced by the same information must be the same and the digital summary produced by different information must be different, which is like human fingerprints. Digital summary is also known as digital fingerprints. The application principle of digital summary is that the sender sends the original information and the digital summary produced by the original information to the receiver, the receiver computes the received original information by the same algorithm and produces digital summary which will be compared to the received digital summary. If the new digital summary is the same as the original information, it means the original information is not changed in the transmission process. Otherwise, the original information is changed.

Conclusion

Data encryption technology is the basic mean to realize the security of e-commerce transactions. The relevant applying technologies, such as digital envelope, digital summary, digital signature, digital time stamp, digital certificate and security transaction protocol based on data encryption technology realized the confidentiality, integrity and non repudiation of information, as well as the certainty of transaction identity in the security of e-commerce transactions, and standardized all parties involved in e-commerce activities and the application of security technologies. At present, there are still many scholars who continue to study and improve the data encryption technology. With the continued progress, the data encryption technology will better ensure the security of e-commerce and will promote the smooth development of e-commerce.

References

[1] Chen H G. The Analysis and Improving of SET [J]. Journal of Wuhan Technical College, 2003.

[2] Bergdale M. Method and system for electronic ticket validation using proximity detection [J]. 2015.

[3] Renu, Ritu. A Noval Approach on Online Transaction Protocols [J]. International Journal of Engineering Sciences & Research Technology, 2014, 3(7).

[4] Cox M A, Bona J K. Point Of Sale Transaction Device with Magnetic Stripe Emulator and Biometric Authentication: US, US20080126260 [P]. 2008.

[5] Gupta H, Sharma V K. Role of Multiple Encryption in Secure Electronic Transaction [J]. International Journal of Network Security & Its Applications, 2011, 3(6).

[6] Dehaan M P, Likins A K, Vidal S K. Systems and methods for secure distributed storage: US, US 8375223 B2 [P]. 2013.

[7] Clark J, Hengartner U. On the use of financial data as a random beacon[C]// International Conference on Electronic Voting Technology/workshop on Trustworthy Elections. USENIX Association, 2010:1-8.

[8] Camp L J. Identity in Digital Government [J]. Ssrn Electronic Journal, 2004.

[9] Xu K, Guo Y, Guo L, et al. My Privacy My Decision: Control of Photo Sharing on Online Social Networks [J]. IEEE Transactions on Dependable & Secure Computing, 2015:1-1.

[10] Tam J W O. Method for making secured personal identity card and procedures for validation and obtaining secure personal information: US, US6968457[P]. 2005.

[11] Colvin Sr. B. Centralized secure communications system: US, US6041123[P]. 2000.

[12] Kang J, Shilton K, Estrin D, et al. Self-Surveillance Privacy[J]. Social Science Electronic Publishing, 2010, 97(3):809-847.