Public-Key applications in E-commerce

Zhaoqing Wang\textsuperscript{1,*}, Yusheng Zhao\textsuperscript{1,b}, Guorong Zhong\textsuperscript{2,*}

\textsuperscript{1} School of Information\textsuperscript{&} Communication Engineering, Beijing Information Science\textsuperscript{&} Technology University, Beijing, China
\textsuperscript{2} International School, Beijing University of Posts and Telecommunications Beijing, China

*Corresponding author email: 2016213302@bupt.edu.cn
mj741561@163.com; zhaoyusheng@bupt.edu.cn

Abstract: In this paper, we describe the application of data encryption technology in E-commerce, and introduce the public key encryption and public key encryption system in detail. Then, we propose a composite encryption model that nests the DES algorithm in the RSA algorithm. Finally, we analyzed two widely used Internet protocols, SET and SLL, which can improve the security of payment and customer trust, and then describe the development of e-commerce by ensuring the security and accuracy of the transaction process.

1. Introduction
With the development of Internet technology, the pattern of online transactions has become increasingly diversified. E-commerce has become the main trading method on the Internet, and it has penetrated into each areas of society at an extreme rate. At the same time, the security of data on the E-commerce platform is also facing unprecedented challenges. The key to data security is confidentiality, integrity and non-repudiation. Data encryption technology has attracted much attention as an active security defense strategy, which provides considerable security protection for information at a small cost. But traditional data encryption methods and Internet protocols are difficult to play a security role in the era of big data. This paper introduces the public key cryptosystem (RSA algorithm) in detail, and proposes a mechanism to nest the DES algorithm under the RSA algorithm, although DES does not belong to the public key cryptosystem (belongs to the symmetric cryptosystem). But nesting it under RSA can better protect the security of E-commerce activities. On the basis of encryption technology, combined with the public key technology of SSL protocol (Secure Sockets Layer Protocol) and SET protocol (Secure Electronic Transaction), the communication confidentiality and transaction credibility on the E-commerce platform can be improved. This paper makes a detailed statement on the application of public key algorithm and related protocols in E-commerce, and proposes optimization, which can intercept the intruder in time. The method is to improve the security defense capability of E-commerce through a higher encryption level.

2. Background

2.1 Public-key Encryption
Encryption is the process of converting readable information called "plaintext" into unreadable information, that is, "ciphertext"; The basic functions of encryption: (1) Prevent uninvited guests from viewing confidential data files; (2) Prevent confidential data from being leaked or tampered; (3) Prevent
privileged users (such as system administrators) from viewing private data files; (4) Make intruders unable to easily find them A system file. Decryption is the process of reversing encrypted information and restoring it to "plaintext ". Both encryption and decryption are performed by cryptographic algorithm. The more complex the cryptographic algorithms are, the safer the ciphertext is. This paper focuses on the public key encryption system.

The public key encryption system, also known as the double-key encryption system, which refers to a cryptosystem in which the encryption key and the decryption key are two different keys. It uses a pair of keys: one is called a public key which is public using by others, and its role is to encrypt or verify the digital signature; the other is called private key which is confidential in order to decrypt information or digitally sign the information. The relationship between these two keys is that the information encrypted with either of these keys can only be decrypted with another one. If using the public key as the encryption key, and using the private key as the decryption key, the information encrypted by one user can be interpreted by multiple users. The former is used for digital encryption, the latter is used for digital signature. The typical public key cryptography algorithms are RSA, ElGamal, backpack algorithm, etc. whereas this paper only states the most commonly used RSA algorithm, and applies it to E-commerce field.

The public key encryption system, also known as the double-key encryption system, which refers to a cryptosystem in which the encryption key and the decryption key are two different keys. It uses a pair of keys: one is called a public key which is public using by others, and its role is to encrypt or verify the digital signature; the other is called private key which is confidential in order to decrypt information or digitally sign the information. The relationship between these two keys is that the information encrypted with either of these keys can only be decrypted with another one. If using the public key as the encryption key, and using the private key as the decryption key, the information encrypted by one user can be interpreted by multiple users. The former is used for digital encryption, the latter is used for digital signature. The typical public key cryptography algorithms are RSA, ElGamal, backpack algorithm, etc. whereas this paper only states the most commonly used RSA algorithm, and applies it to E-commerce field.

In E-commerce area, in order to use the public network to trade with thousands of customers, the public key cryptosystem is a good choice, it is very secure and difficult to crack. For single-key encryption systems for electronic trading merchants, public key cryptosystems have irreplaceable advantages. Since the encryption key is public, the key distribution and management is simple to be implemented. For example, only one key is needed for a multiple-user network. However, data security has also formed as a big trial, so a comprehensive encryption algorithm is essential to ensure data security and privacy.

2.2 Public Key Infrastructure
The public key infrastructure is a universal secure infrastructure that implements and provides security services using public key concepts and technologies. In addition to encryption, decryption, and key management, it also includes various security policies, security protocols, and security services. PKI technology is the core of information security technology and the essential technology of E-commerce. A complete PKI system should have basic components like the authoritative certification authority (CA), digital certificate library, key backup and recovery system, certificate invalidation system, and application interface (API). The construction of PKI will also be built around these five systems.
Figure 3. Public Key Infrastructure structure

PKI, a key cryptographic technology, is widely used in open network-based E-commerce systems. As a foundation for E-commerce security, it enhances the security service functionalities, such as authentication, confidentiality, integrity, and non-repudiation of the systems.

3. The application of RSA Algorithm in E-commerce

Encrypting the file only solves the problem of confidentiality of the transmitted information. And we need other measure to prevent others from destroying the transmitted files and how to determine the identity of the sender, which is digital signature. In the E-commerce security system, digital signature technology has a particularly important position. Digital signature technology is used in source authentication, integrity services, and non-repudiation services in E-commerce security services. The most widely used digital signature method is the RSA algorithm.

3.1 RSA algorithm — asymmetric encryption

The RSA algorithm was first proposed by Shamir, Adelman in 1978. RSA uses a combination of a public key and a private key. The public key is represented by PK, and the private key is represented by SK. In the encryption process, the plaintext needs to be divided into blocks, the size can be changed, and the length is limited, and the key length must not be exceeded. The algorithm converts the plaintext represented by the block into a ciphertext of the same length as the key. The following describes the process of the RSA algorithm:

1. Determine the two confidential heterogeneous prime numbers, take p, q, and let n = pq, calculate r is a number that is mutually prime with \((p-1)(q-1)\), let r represent SK;
2. Let a value be m such that \(rm = 1 \mod (p-1)(q-1)\);
3. According to the Euclidean algorithm \((a = bn + c, \text{ then the } \gcd \text{ of } a \text{ and } b \text{ are equal to the } \gcd \text{ of } b \text{ and } c)\), the solution is m, and the obtained m and n are the public key PK;
4. In the encoding process, it is assumed that the data is set to A, and the plaintext is divided into N data blocks of equal length, assuming \(a < n\), thereby calculating \(b = a^m \mod (pq)\), that is, b is the obtained data after encoding;
5. In the decoding process, let \(c = b^r \mod (pq)\), and get \(c = a\).
Figure 4. RSA algorithm encryption and decryption process

In the E-commerce platform, if the intruder wants to crack r, the necessary premise is to expand the factorization of n. So it is necessary to select a large index p, q to prevent the criminals factoring. In short, the security level of the E-commerce platform depends on the size of the prime number, and the security level of the RSA is determined by the large exponential decomposition.

3.2 Optimization based on RSA algorithm

This paper proposes an idea of nesting encryption algorithms. Although DES does not belong to the public key cryptosystem, but nesting it under the RSA algorithm can better ensure the security of E-commerce activities. Compared with the RSA algorithm, the DES algorithm has the advantages of algorithm disclosure, small amount of calculation, fast encryption speed, high encryption efficiency, and unlimited plaintext length. However, both parties to the transaction use the same key, security is difficult to guarantee, and in terms of key storage, it possibility has the problem of key is leaked and stolen as long as there is transmission. In the communication process, the RSA algorithm does not need to exchange keys in advance, which is beneficial to the reasonable allocation and effective management of the key. And the public key can generate a digital signature, which can ensure the uniqueness of the identity of the information transmitter in the E-commerce. However, the length of the plaintext is limited when encrypted with RSA, and in practice the length of the plaintext we want to encrypt may be longer than the length of the key. This uses a nested approach that combines the advantages of both algorithms.

3.3 RSA digital signature system

The digital signature technique in the RSA algorithm is actually implemented by a hash function. A feature of digital signatures is that the characteristics of a document is represented by it. If the file changes, the digital signature value will change at the same time. The different file will be arranged different digital signature. A simplest hash functions is to accumulate the binary code of a file and take the last few bits. The Hash function is public to both sides of the transmitted data. Adding digital signatures to E-commerce platforms can achieve secure transmission over public networks.

For example, in an E-commerce transaction, if a third party pretends to be a merchant and issue a transaction file, because the client uses the public key of the merchant when decrypting the digital signature. As long as the third party does not know the private key of the merchant, the decrypted digital signature and the calculated digital signature are necessarily different. This provides a secure way to confirm the identity of the business.

4. The application of Internet Protocol in E-commerce

To ensure the smooth conduct of E-commerce transactions, the following requirements must be met: (1) the uniqueness and authenticity of the identity of both parties in the transaction; (2) the privacy of the data of the communicating parties; (3) The validity and authenticity of the E-commerce transaction order information; (4) the non-repudiation of the order information of the parties in the transaction; (5) the
authority of the third-party fair ruling. Undoubtedly, ensuring the environmental security of the transaction process is essential, and data encryption technology is an effective measure.

4.1 The payment information security
The SET protocol ensures the payment information is safe and effective in the e-commerce BtoC mode. SET payment system participants mainly include: cardholders, merchants, card issuers, receiving banks and payment gateways. In addition, it also involves the Certification Authority(CA). The CA issues a specific certificate to each participant in the SET payment system, aim to determine whether the other party is safe and trustworthy. To have a secure and dependable E-commerce payment system, it is indispensable to establish a certification body with strong qualifications and high confidence. The idea of the optimizing algorithm mentioned above is combined with the SET protocol, in which the public key encryption uses the RSA algorithm and the private key encryption algorithm is the DES data encryption standard.

4.2 The trust in online trading
The establishment of transaction trust is crucial. The trust of customers means that the company have earned profits. The SSL protocol can enhance the trust of online transactions and ensure the security of data information in transactions.

The SSL security protocol provides the following services in E-commerce: (1) Verify that the user and server are legitimate. This ensures that data information is sent to a secure and correct server; (2) the encryption technology used includes both symmetric key technology and public key technology. First exchange SSL initial handshake information. Before the server and client exchange data, the handshake information is encrypted by encryption technology to ensure the confidentiality and accuracy of the data. Then use digital certificates to identify and prevent intruders deciphering[5]; (3) SSL establishes a secure channel to connect between the server and client. The encryption technology used is Hash and secret sharing. This ensures the accuracy and security of the data information. And ensure that each service entering the secure channel can reach the designated location accurately during the transmission.

5. Conclusion
This paper first introduces the public key encryption and public key encryption system, and discusses the application of data encryption technology in business activities based on E-commerce. The RSA public key encryption algorithm is introduced in detail, and an encryption model based on RSA algorithm is proposed. Finally, the two most widely used SET and SSL protocols in the E-commerce process are described, which ensures the security of payment information and improves the trust of online transactions. Public key encryption technology is the guarantee of E-commerce security. We can only continue to promote the development of E-commerce by ensuring the security and accuracy of the transaction process.

Reference
[1] W. Stallings, Cryptography and network security. Upper Saddle River: Prentice Hall, 2014.
[2] Weng Yunxiang. Research and design of hybrid encryption algorithm based on DES and RSA [J]. Electronic Design Engineering, 2016(9): 165-168.
[3] Wei Wei, Wang Chen, Li Xingyi. Application of Express Information Privacy Protection Based on RSA Algorithm[J]. Information Security, 2014(7): 43-45.
[4] Ru Ruxian. Data Encryption Technology and Its Application in E-commerce [J]. Microcomputer Information, 2010(10): 38-41.

[5] Wang Yi. Implementation of Data Encryption Transmission in Electronic Commerce [J]. Dandong Textile Institute, 2005(6): 25-29.

[6] Saxena S, Kapoor B. An efficient parallel algorithm for secured data communications using RSA public key cryptography method [C]. Advance Computing Conference (IACC), 2014 IEEE International.

[7] Klaus Hansen, Troels Larsen, Kim Olsen. On the Efficiency of Fast RSA Variants in Modern Mobile Phones [J]. International Journal of Computer Science and Information Security, 2009, 6(3).

[8] Satyanarayana Vollala, Varadhan V V, K. Geetha et al.. Design of RSA Processor for Concurrent Cryptographic Transformations [J]. Microelectronics Journal, 2017.