E-book shopping System with Cryptography by using RSA Algorithm

Ei Mon Kyaw
Computer Studies (Pathein)
minminzaw67@gmail.com, mayphyooo@gmail.com

Abstract

This paper presents e-book shopping system with cryptography by using RSA algorithm. Information security is a major issue today for any company or individual who conducts business electronically. Computer applications need to protect their data from an unauthorized access. The most important security tool is cryptography. Cryptography provides stronger methods of authentication, called digital signatures and certificates. Public Key Cryptography can be used for confidentiality, authentication, or both. Digital signature is a user authentication method to prevent impersonations .The proposed system utilizes the combination of public key cryptography (RSA) algorithm and secure hash algorithm (SHA-1). In this system, cryptography is used in encryption of order information and payments information of customer and market.

Key Words: Cryptography, RSA, Digital Signature, Secure Hash Algorithm

1. Introduction

Cryptography is the art of secret writing. Because of the development of electronic commerce, cryptographic techniques are extremely critical to the development and use of defense information systems and communications networks. So, protection of data from unauthorized parties is essential. Cryptography [9] is the science of protecting data, which provides means and methods of converting data into unreadable form.

The data cannot be accessed for unauthorized use. The content of the data frames is hidden. The authenticity of the data can be established. The undetected modification of the data is avoided. The two main encryption techniques are symmetric encryption and asymmetric encryption. Symmetric encryption technique is based on a single key also known as symmetric key or private key or secret key encryption. Asymmetric encryption is based on a combination of two keys, public key and private key. Asymmetric public key cryptography is used in this system [1].

Public key cryptography is used to protect digital data going through an insecure channel from one place to another. The RSA idea can also be used for signing and verifying a message is called the RSA digital signature scheme. The digital signature scheme changes the roles of the private and public keys. First, the private and public keys of the sender, not the receiver, are used. Second, the sender uses her own private key to sign the document: the receiver uses the sender's public key to verify it. If we compare the scheme with the conventional way of signing, the private key plays the role of the sender's own signature; the sender's public key plays the role of the copy of the signature that is available to the public [8].

This paper presents implementation of e-book shopping system with the RSA algorithm and is organized as follows: section 1 introduces the system, section 2 explains block cipher and stream

cipher of the system and section 3 in this paper contributes as securing transactions of the system. And then, section 4 discusses the system design and implementation and section 5 presents explains conclusion. Finally, the last section is references.

2. Related Work

One of the main categorization methods for encryption techniques commonly used is based on the form of the input data they operate on. The two types are Block Cipher and Stream Cipher [2].

The most encryption algorithms operate on fixed-size blocks of data; 64 bits is a popular size for the blocks. A message is subdivided into blocks; the last block is padded to the standard length if necessary and each block is encrypted independently. The first block is available for transmission as soon as it has been encrypted. The four significant characteristics of a model are: parallelization, Initialization vector, error propagation, and self-synchronizing.

In a stream cipher, encryption and decryption are done one symbols at a time. Stream ciphers are classified into two types: synchronous stream ciphers and asynchronous stream ciphers. Most notably, they are usually faster and have a lower hardware complexity than block ciphers [9].

3. Securing Transactions

Online transactions typically require: message integrity to ensure messages are unaltered during transit; message confidentiality to ensure message content remain secret; non repudiation to ensure that the sending party cannot deny sending the received message; and sender authentication to prove sender identity.

3.1 Symmetric Cryptography

Symmetric cryptography tries to ensure message confidentiality by encrypting the message (the plaintext) using a secret key to produce an encrypted version of the message (the cipher text), which is then sent instead of the original message. Message integrity is implicitly provided, as altering the cipher text would result in an illegible decrypted message.

'Symmetric' refers to the fact that the same secret key is required to decrypt the message on the recipient's side. Typical symmetric encryption algorithms include DES, Triple DES, RC2, RC5, Twofish, Blowfish, IDEA and AES. Most symmetric algorithms can operate in two modes, namely Cipher Block Chaining Mode (CBC) or Electronic Codebook Mode (ECB) [3].

3.2 Asymmetric Cryptography (public key cryptography)

Asymmetric cryptography provides the same message security guarantees as symmetric cryptography, but additionally provides the non-repudiation guarantee. 'Asymmetric' refers to the fact that different keys are used for encryption and decryption. One key is kept secret ('secret key') and the other is made public ('public key'), and are both unique. The recipient's public key should be used during the encryption process to ensure message confidentiality as only the recipient has the necessary secret key to decrypt the message. If, however, the message is encrypted using the sender's private key the sender cannot deny sending the message as his private key is unique and is only known to him. Typical asymmetric algorithms include RSA, ElGamal and DSA. Asymmetric cryptography is extremely powerful, but this comes at a cost. Especially for longer messages and keys, it is much slower than its symmetric cryptography counterparts.

3.3 RSA Encryption and Decryption Algorithms

Given the public key e and the modulus n, the private key d for decryption has to be found by factoring n. Choose two large prime numbers, p and

q, and compute the modulus n which is the product of two primes: n = p q choose the encryption key e : e and φ(n) are co prime, i.e. gcd (e, φ(n)) = 1, in which φ(n) = (p − 1)(q − 1) is called Euler's totient function. Using Euclidean algorithm, the private key d for decryption can be computed by taking the multiplicative inverse of e such that $d = e^{-1} \pmod{\varphi(n)}$ or $ed = 1 \pmod{\varphi(n)}$. The decryption key d and the modulus n are also relatively primed. The numbers e and n are called the public keys, while the number d is called the private key.

To encrypt a message m, the cipher text c corresponding to the message block can be found using the following encryption formula: $c = m^e \pmod{n}$.

To decrypt the cipher text c, c is raised to the power d in order to recover the message m as follows: $m = c^d \pmod{n}$.It is proved that $c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n = m \pmod{n}$due to the fact that $ed = 1 \pmod{\varphi(n)}$ [7].

3.4 RSA Digital Signature Algorithm

The RSA public-key cryptosystem can be used for both encryption and signatures. Each user has three integers: e, d and n, n = p q with p and q large primes. For the key pair (e, d), $ed = 1 \pmod{\varphi(n)}$ must be satisfied. If sender A wants to send signed message c corresponding to message m to receiver B, A signs it using A's private key, computing $c = m^{dA} \pmod{n_A}$. First A computes $(n_A) = (p_A - 1, q_A - 1)$. The sender A selects his own key pair (e_A, d_A) such that $e_A.d_A = 1 \pmod{(n_A)}$. The modulus nA and the public key e_A are published [5].

3.5 Secure Hash Algorithm

There are several hash algorithms such as MD2, MD4 and MD5, where MD stands for Message Digest and SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512, where SHA stands for Secure Hash Algorithm. These algorithms enable the determination of a message's integrity: any change to the message will, with a very high probability, results in a different message digest. This property is useful in the creation and verification of digital signatures and message authentication codes, and in the generation of random numbers (bits). Algorithm can be described in two stages: preprocessing and hash computation. Preprocessing involves padding a message, parsing the padded message into m-bit blocks, and setting initialization values to be used in the hash computation. The hash computation generates a message schedule from the padded message and uses that schedule, along with functions, constants, and word operations to iteratively generate a series of hash values. The final hash value generated by the hash computation is used to determine the message digest.

4. System Design and Implementation

We have implemented the secure e-book shopping system to prevent information from access by unauthorized parties, while it is being transmitted, which is when it is most vulnerable to interception. It also guarantees authenticity by using RSA digital signature and secure hash algorithm. If a document itself has been altered in any way during transmission, the two hash code will not match at the recipient, and it can also provide "non-repudiation" of transmitted information. The system uses a 1024-bit modulus RSA and secures hash algorithm (SHA-1) implementation, which is adequate for shopping system [4].

4.1 System Design

In this system, all of three (customer, market and bank) sites generate the public and private key pairs by using RSA key generation algorithm and sends the public key to other site. All sites maintain their own key pairs and other's public key. The following activities are included key generation by using RSA, key distribution to other sites, sending request, process request and response in this system.

After the key generation and sending have established, Customer site sends to Market it's buying items and own account for order by using digital signature with hashing. Market site decrypt and verify the receiving data pack (cipher and signature) and sends to Bank that the Customer's account and its own account for transfer amount. Bank site also decrypt and verify the receiving data pack (cipher and signature) and processed it. If the process is successful, Bank replies to Market that the process is successful and Market also reply to Customer. If the process fails, Bank reply to Market that the process fails and Market also reply to Customer. Figure 1 shows flowchart of the system design.

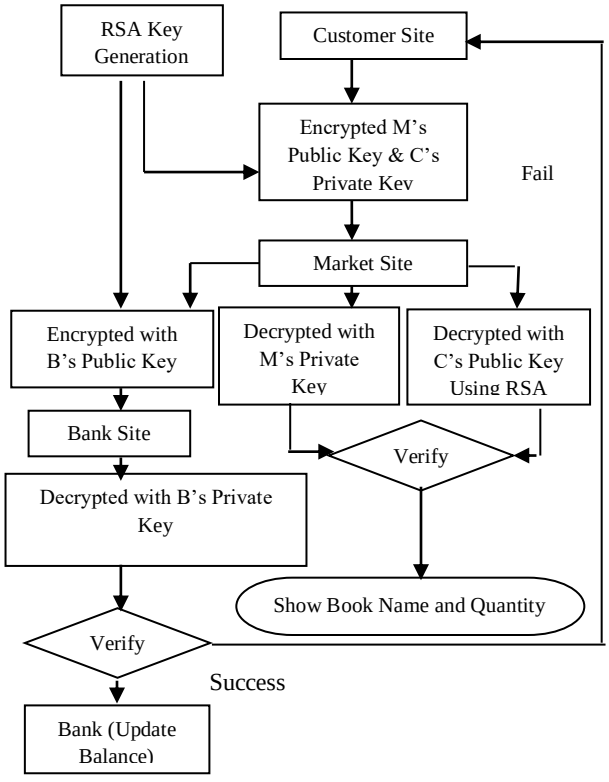

Figure 1 Flowchart of the System Design

4.1.1 Customer Site

The customer creates a message and generate 64-bits message digest by using SHA-1. The message digest is digitally signed by using the customer's private key to produce a signature. The customer also encrypts that original message by using the market's public key to produce an encrypted message. The sender concatenates a signature and an encrypted message and send to the market as a data pack.

4.1.2 Bank Site

Bank decrypts the market account cipher with bank's private key. Bank decrypts the customer payment cipher with bank's private key. Bank also decrypts a signed message by using the customer's public key to produce a original message digest. The bank generates 64-bits message digest by using SHA-1 on that original message. If the two messages digest match, verification complete and check the customer account, and update the balance of customer and market account. If the customer account is not enough to buy the e-book, bank reply to customer the process is fail.

4.1.3 Market Site

The market decrypts a signed message by using the customer's public key to produce a message digest. After recovering the signature, the market also decrypts the encrypted message by using the recipient's private key to produce the original message. The recipient generates 64-bits message digest by using SHA-1 on that original message. If the two messages digest match, verification complete and the message is accepted. The market encrypts the market account send it to the bank with the customer data pack.

4.2. Implementation of the System

This system presents the graphical user interface which integrated in the system to make the

activities of the system. The graphical user interface is described for each activity. In this system, there are three sites: customer site, market site and bank site.

4.2.1Customer Site

The interface of Customer site displays he key generation and key sending are the pre-process of the system. The interface of order form is shown in Figure 2.After the key generation and sending have finished, according to the order form Customer sent the data pack which contains order information cipher that encrypts with Market's public key and account number cipher that encrypts with bank's public key and signature that signs with its own private key to Market site bank's site. Customer site encryption form is shown in Figure 3.

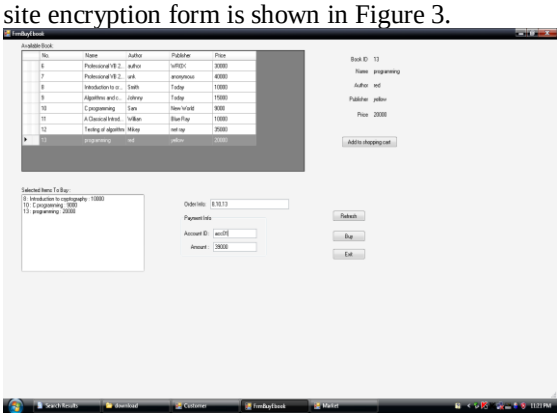

Figure2. Customer Site Order Form

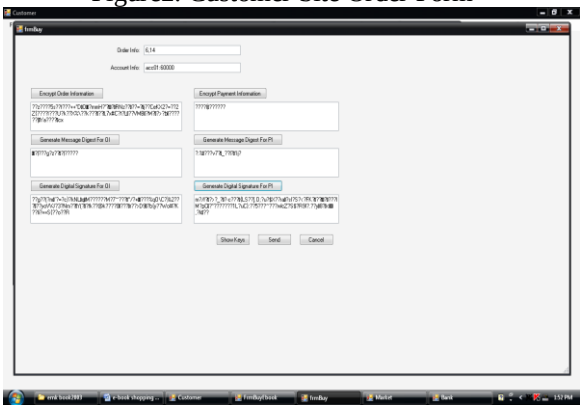

Figure 3.Customer Site Encryption Form

4.2.2 Market site

The interface of Market site displays the key generation step under file menu and order receive step under Receive menu. The interface of receive data from customer form in Figure 4. Market has received the data pack which contains cipher and signature and decrypts the cipher with own private key and verify the signature with the Customer's public key. From this form Market site sent to Bank that its own account and received Customer's account and amount as a data pack for transfer amount. Market site upload e-book form is show in Figure5.

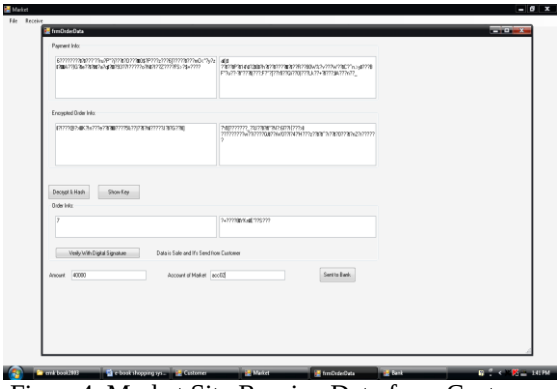

Figure4. Market Site Receive Data from Customer form

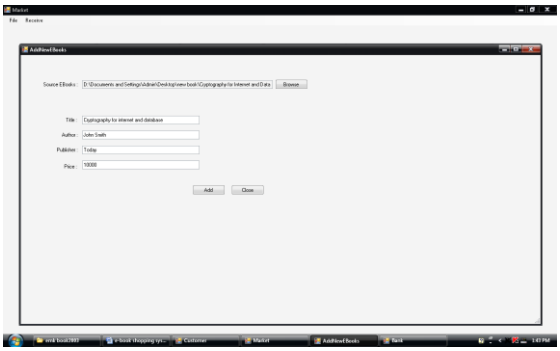

Figure5. Market Site Upload E-book Form

4.2.3 Bank site

Bank site also displays the key generation step under file menu and receive data from Market step

under data menu. The interface of receive data from According to these interface, Bank site receives the data pack which contains cipher and signature and decrypts the cipher with own private key and hash and verify with the Market's public key. After that Bank site processes the transfer transaction and returns to the Market site that the process is successful or unsuccessful. Market site also returns to the Customer site that is successful or unsuccessful.

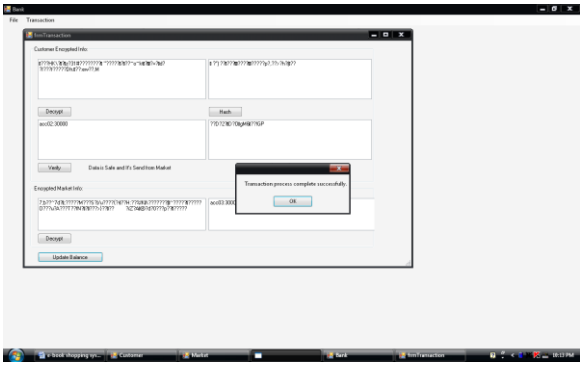

Figure 6. Receive Data and Process Form of Bank Site

6. Conclusions

In this paper, we implemented e-book shopping system using RSA digital signature and SHA-1.The proposed system provides secure protect the falsification and modification of message by third party. Therefore, using the digital signature and hashing provides authentication to establish identity of sender and ensure that message contents are not altered. Our e-book system supports protecting buyer's buying products and personal account information for customer, market and bank by using RSA digital signature algorithm. Therefore, using the digital signature and hashing provides authentication to establish identity of sender and ensure that message contents are not altered.

7. References

[1] A. Hiltgen, T. Kramp and T. Weigold, "*Secure Internet Banking Authentication*", Published by the IEEE Computer Society.

[2] B.A.Forouzan, "*Cryptography and Network Security*", International Edition, 2008.

[3] C.lamprecht, A. van Moorsel, P. Tomlinson and N. Thomas, "*Investing the Effienciency of Cryptographic Algorithm in OnlineTranscations*", University of Newcastle upon Tgne, UK.

[4] Federal Information, "*Secure Hash Standard"*, Processing Standards Publication 180-2, Aug 1, 2002.

[5] P. Kitsos, N. Sklavos and O. Koufopavlou, "*An Efficient Implementation of the Digital Signature Algorithm"*, VLSI Design Laboratory, Electrical and Computer Engineering Department, University of Patra , Patras, GREECE.

[6] Q. Dang, "*Randomized Hashing for Digital Signatures"*, Computer Security Division, Information Technology Laboratory, Aug 2008.

[7] R. Kightlinger, "*Number Theory, RSA Encryption Algorithm"*, May 2, 2005.

[8] R.L Rivest, A. Shamir, and L. Adleman, "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Laboratory for Computer Science, Massachusetts Institute of Technology*.

[9] W.Stallings, "*Cryptography and Network Security*", Principles and Practices, Fourth Edition, 2006.