Online Money Transfer System Using ElGamal Digital Signature Scheme

Sandar Moe, Zin May Aye
University of Computer Studies (Mawlamyine) Myanmar
moesatt04@gmail.com, zinmay110@gmail.com

Abstract

This paper presents money transfer transaction from bank to bank system to provide authentic, integrity services by using ElGamal public key digital signature and SHA-512 hash function algorithm. This system consists of two components: Signing and Verifying. Signing process is performed by sender and verifying process is performed by receiver. In signing process, administrator creates signature with its private key and send its signature & original ticket to other administrator. In receiving process, administrator computes hash code from original ticket and compares hash code from decrypted signature with its public key. The security of ElGamal signature algorithm is based on computing discrete logarithm over a finite large prime. The security of SHA-512 is large size of digest output. If two hash values are equal, the content of ticket message is not modified after signed and display ticket message of money transfer is successful. If two hash values are not equal, the content of ticket message is modified after signed.

Keywords: Digital Signature, ElGamal digital signature, SHA-512, Authentication, Integrity

1. Introduction

Applications of digital signature technology are on the rise because of legal and technological developments, along with the strong market demand for secured transactions on the Internet. Information security is needed to cover the most of threads over the network. Information security means not only for storing and communication data in secrete but also for ensuring that the source of message is valid and the message has not been altered. Digital signature is rapidly becoming ubiquitous in many aspects of electronic life [7]. They are used to obtain security services such as authentication, data integrity and non-repudiation. Digital signature schemes can be used for sender authentication and non-repudiation. In this paper, security of online banking system is implemented by using Elgamal and SHA-1 algorithm. Elgamal signature algorithm is used for key generation, signature generation and signature verification. Integrity is one kind of security and it means that the information cannot be altered in storage or transit between sender and intended receiver without the alternation being detected. Authentication is that the sender and receiver can confirm each other's identity and the origin or destination of the information.

Digital signature software enables you to easily migrate from cumbersome paper-based processes to a secure and efficient paper-free environment [2]. Digital signature mechanism can be implemented by combining public key cryptography and hash function [4,5]. Digital signature can resolve the problem because of its data integrity protecting and privacy. A hash function H is a transformation that takes an input m and returns a fixed-size string, which is called the hash value h that is, h = H(m) [3]. System uses two algorithms: one is signing in which a private key is used to process the message and another is verification in which the matching public key is used with the message to check the validity of the signature.

With digital signature technology, any change in the signed ticket message causes the verification process to fail. This paper presents implementation of online money transfer system with the ElGamal signature algorithm and is organized as follows: section 1 introduces the system, section 2 presents related works, section 3 explains theory background of the system. And then, section 4&5 discusses the system design and implementation and section 6 explains user interfaces, section 7 explains conclusion, section 8 explains result and discussion of the system.

2. Related Works

Information security algorithms using ElGamal for signature generation and verification are applied in real world system such as electronic mail, electronic funds transfer, electronic data interchanges, software distribution, data storage, and other applications which require data integrity assurance and data origin authentication [3].

The author Steve Burnett & Stephen Paine write about the digital signature and secure data encryption by using RSA and ElGamal algorithm in the RSA Security's Official Guide to Cryptography book. The author Jim Minihan research about digital signature by most useful signature algorithm DSA, ElGamal, RSA and ECDSA.

Brian Bladman, Carl Ellison and Nicholas Bohm proposed digital signatures, certificates and electronic commerce [1]. This system can further extend to give non-repudiation services by applying certificate authority (CA) as a third party between bank administrators. It also turns out that digital certificates are more effective as mechanisms for attaching permissions to digital signatures instead of names or identities.

3. Background Theory

In this online money transfer system, digital signature is implemented with ElGamal digital signature scheme and SHA-512 hash function. Signature generation/ verification are explained in detailed in the following sections.

3.1 Secure Hash Function (SHA 512)

SHA-512 is the version of SHA with a 512-bit message digest [4]. It is more complex structure than others, and its message digest is the longest. It is one-way hash function which is fixed output, strongly collision free. SHA-512 is more secure and more efficient than the other hash functions because of using larger digest messages to provide more resistant to possible attacks and to be more secure the system. The algorithm takes as input a message with a maximum length of less than 2^{128} bits and produces as output a 512-bit message digest. The input is processed in 1024-bit blocks.

It is firstly performed append padding bits which is always added, even if the message is already of the desired length. Thus, the number of padding bits is in the range of 1 to 1024 bits. The padding consists of a single 1-bit followed by the necessary number of 0-bits.Then, it processes append length. A block of 128 bits is appended to the message. This block is treated as an unsigned 128-bit integer and contains the length of the original message (before the padding).The outcome of the first two steps yields a message that is an integer multiple of 1024 bits in length. The total length of the expanded message is N x 1024 bits. Initialize hash 512 bits buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as eight 64-bit registers (a, b, c, d, e, f, g, h). These registers are initialized to the following 64-bit integers (hexadecimal values). It processes message in 1024-bit (128-word) blocks. A single block 1024 bits of number steps is processed 80 round. After all N 1024-bit blocks have been processed; the output from the N^{th} stage is the 512-bit message digest.

3.2 Digital Signature

For message sent through an insecure channel, integrity is guaranteed in public key systems by using digital signature. A digital signature can be used to guarantee, beyond doubt, the validity of message integrity and that of non-repudiation [6]. Public key cryptography and hash function provide a method for employing digital signature. Very often digital signatures are used with hash functions; hash of a message is signed, instead of the message [4]. The signature for a message can only be generated by someone with knowledge of private key. If message is modified in any way, the signature no longer matches. So, digital signatures provide two important functions [7]. They prove who generated the information, and they prove that the information has not been modified in any way by anyone since the message and matching signature were generated. These factors are important in digital signature:

Integrity: The sender and receiver of a message may have a confidence that the message has not been altered during transmission. If a message is digitally signed, any change in the message will invalidate the signature.

Authentication: Digital signature can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was send by that user.

3.2.1. ElGamal Dgital Signature Scheme

The ElGamal signature scheme is a digital signature scheme which is based on the difficulty of computing discrete logarithms [8]. The ElGamal signature scheme must not be confused with ElGamal encryption which was also invented by Taher ElGamal. ElGamal digital signature scheme has three components,

- Key generation
- Signature creation and
- Signature verification

Key Generation

A prime p of length 512 bits is chosen first.

- Let e_1 be a generator of Zp*.
- Pick d in [2, p-2] at random.
- Compute $e_2=e_1^d \bmod p$.
- Public key: p, e_1, e_2
- Private key: d.

Signature Creation

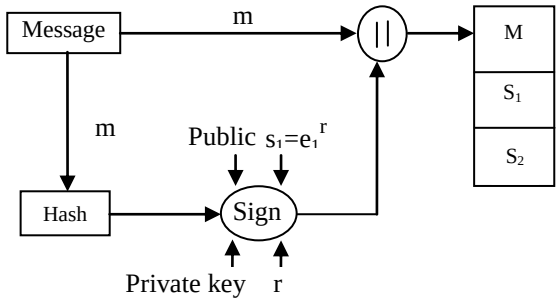

Figure 1: ElGamal Signing Process

In this process, r is chosen. Sender needs a new r each time it signs a new message. Let m=H (M). Pick r in [1, p-2] relatively prime to p-1 at random.

- Compute $s_1=e_1^r \bmod p$.
- Compute $s_2= (H(M)-s_1d)r^{-1} \bmod (p-1)$
- Output s_1 and s_2.

Signature Verification

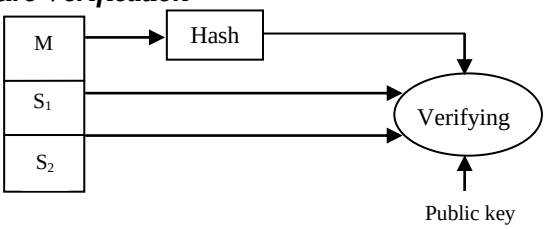

Figure 2:ElGamal Verifying Process

In this process, receiver receives M, s_1 and s_2 which can be verified as follows:

Receiver checks to see if $0 < S_1 < p$. and $0 < S_2 < p$-
Calculate $v_1 = e_1^{h(m)} \bmod p$, $v_2 = e_2^{S1} S_1^{S2} \bmod p$. If V_1 is congruent to V_2, the message is accepted; otherwise, it is rejected.

4. Implementation of the System

In this money transfer system, users' information is created as a ticket by the bank's administrator. Before creating the ticket, administrator firstly needs to login to enter online money transfer system. Each administrator must have correct name/password to process the system. Then, he/she creates ticket with customer information and checks the ticket.

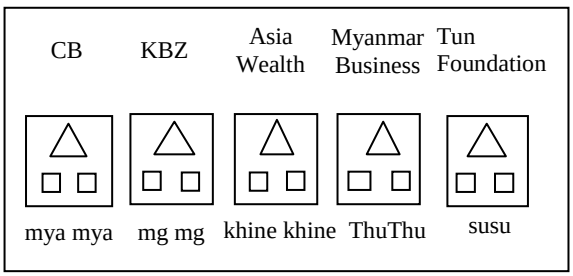

Figure 3: Banks and their Respective Administrators

Bank administrators can connect with each other to process online money transfer system. In this system, some of banks name and their respective administrator are shown as in figure 3. Figure(4) & (5) show the responsibilities of bank's administrator(sender side and receiver side).

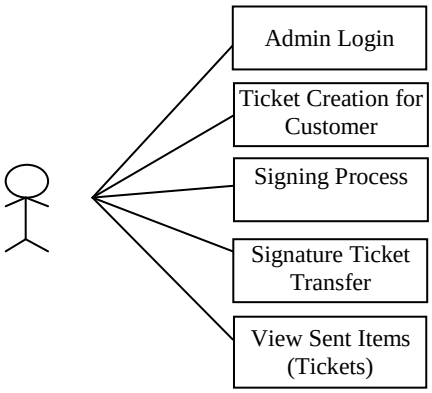

Figure 4: Bank Administrator from Sender Side

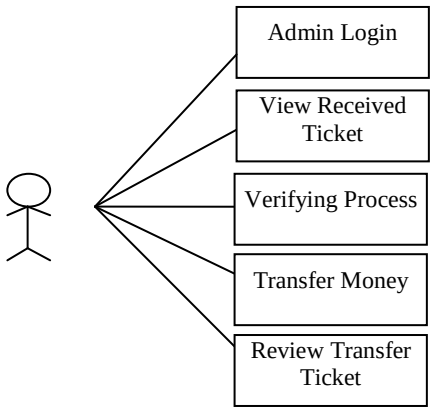

Figure 5: Bank Administrator from Receiver Side

4.1 Security on ELGamal Digital Signature Scheme

In ElGamal digital signature scheme, sender produces a one-way hash function to create a hash value of that original ticket which represents the unique fingerprint for the whole document. The hash value is encrypted using sender's private key and resulting the digital signature. From the view of attacks on ElGamal digital signature scheme, the security of the system rests on the assumption of discrete logarithm and they are difficult to compute for the attackers.

5. System Design

In this system, it mainly consists of two process:

(1) Signing process
(2) Verifying process

Signing Process

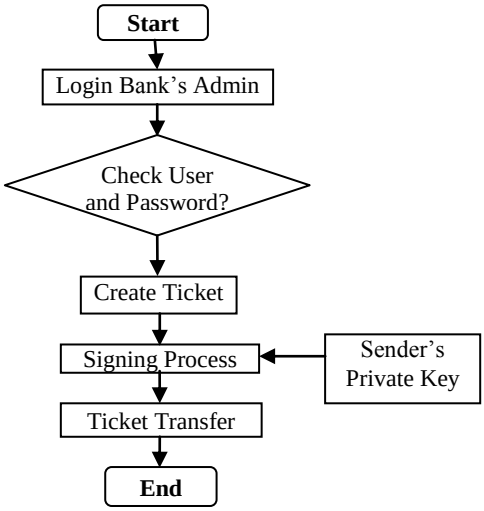

Figure 6: Flow Diagram for Bank Admin (sender side)

In sending process, administrator firstly needs to login to enter online money transfer system. Each administrator must have correct name/password to process system. And administrator performs signing process for customers to ticket form with administrator's private key. The resulting hash value is the digital signature. The digital signature attached with the original ticket is sent to the receiver side as shown in Figure 6.

Verifying Process

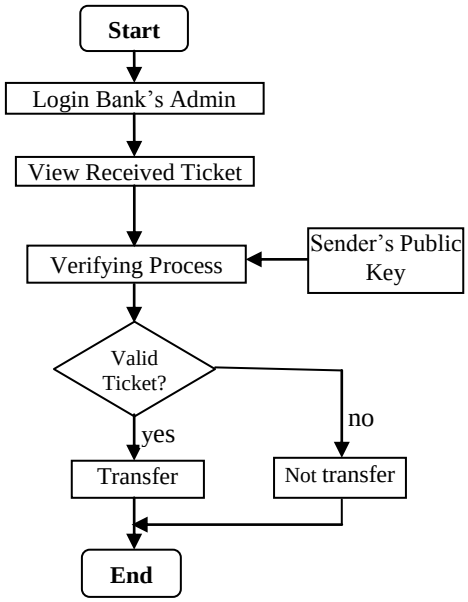

Figure 7: Flow Diagram for Receiver Side

In receiving process, administrator enters login to check sent items from sending. Incoming input is divided into its components: the digital signature and the ticket itself. The administrator's public key is applied to the digital signature. The result of the values is then verified with the hash value of the original ticket. If the ticket is true, money transfers system is valid.

5.1. System Flow Diagram

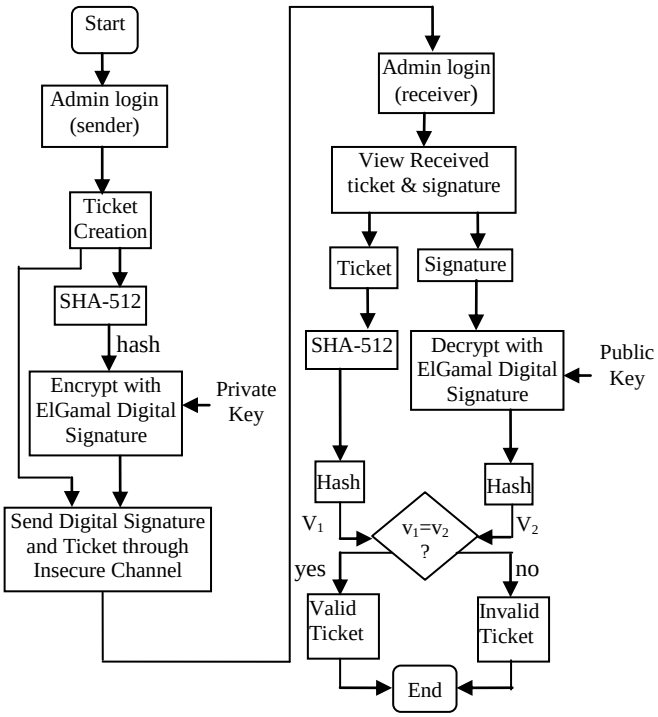

Figure 8: System Flow Design for Money Transfer System

Figure 8 shows system flow for online money transfer system. First, administrator enters login to the money transfer form. And then, administrator must to fill money transfer form and the system computes hash value of ticket message using SHA-512 hash algorithm. This is ticket integrity. Second, system encrypts hash value with signer's private key using ElGamal digital signature algorithm. The output is digital signature of the original input. Finally, digital signature is attached to the ticket message and the whole data is sent to the receiver pass over insecure channel.

Receiver accepts the ticket message and extracts the digital signature. Then, receiver decrypts the digital signature with signer's public key using ElGamal digital signature algorithm and computes hash value of ticket using the SHA-512 algorithm. Bank administrator compares the two hash values. If the two hash values (v_1&v_2) are equal, the ticket was not modified and sent by valid sender. This is ticket authentication. If the two hash values (v_1&v_2) are

not equal, the ticket was modified and sent by invalid sender.

6. Implementation for User Interface

This section describes implementation of user interfaces for online money transfer system. Firstly, Bank administrators' need to login in to the system. Then, he creates ticket with customer information and checks the ticket.

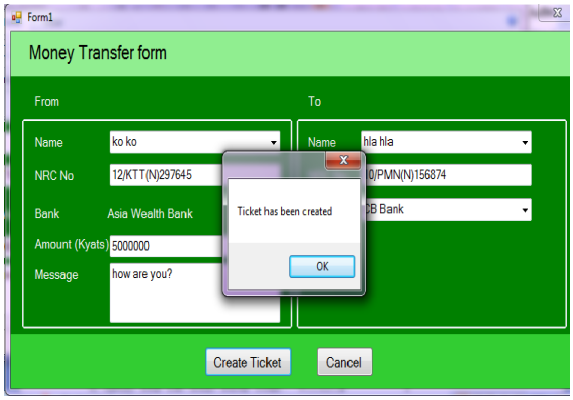

Figure 9: Creating a Ticket

As in figure 9, the creation of a ticket fills up in the customer required field (customers' name, NRC No, money amount, chosen bank and message) to create a ticket.

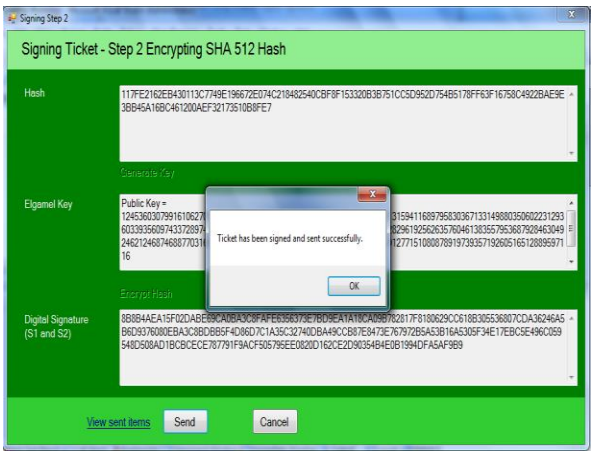

Figure 10: Signature Generation

Figure10 shows signature generation. In signature generation, ticket is firstly hashed with SHA-512. Then, the hash value is signed with ElGamal signature private key. The content of ticket is not modified after signed and was send valid sender.

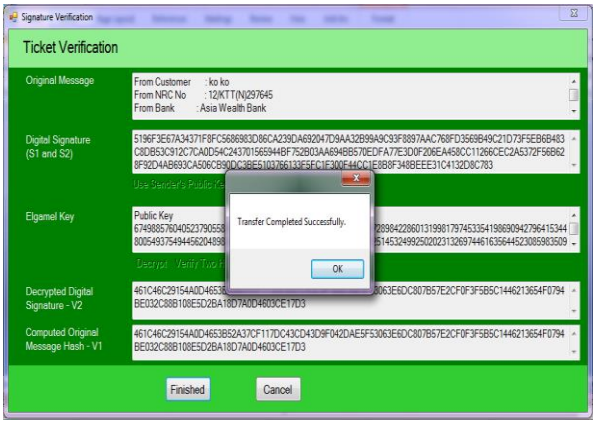

Figure 11: Signature Verification

The hashed ticket and the decrypted signatures are verified to check the validity of a ticket. It is shown as in figure11. If the ticket is not modified during transmission receiver can accept the ticket and online money transfer process is accomplished with having integrity and authentication goals for the implemented system.

7. Results and Discussions

The results for the online money transfer using ElGamal digital signature is discussed with the experimental procedures. For money transfer, the system needs to create a ticket. It consists of amount of money to be transferred, customer name, identity number and message. The authorized bank administrator needs to fill which bank and by whom the ticket is received. By using ElGamal digital signature scheme and performing signing process at the sender side, money transfer would be accomplished. The details of the configuration are shown in figure 10 and 11 in section 6. For the recipient, the authorized bank's admin can verify the validity of the received ticket from sender and can prove authenticity and integrity for the received ticket. The system is based on ElGamal digital signature and so signing and verifying processes are essential tools for sender and receiver respectively to accomplish the online money transfer system.

8. Conclusions

This paper is implemented to apply for online money transfer system by using Elgamal digital signature and SHA-512 algorithm. Using the digital signature and hashing provides the system to achieve authentication for users and ensure the integrity of the transfer message (ticket). In this system, the two main important processes are signing and verifying. Hash value of a ticket is calculated by SHA-512 and output of 512 bits hash code is encrypted ElGamal digital signature algorithm to form a digitally signed message.

Receiving ticket and signature are verified by the authorized bank administrator to check the validity of the ticket by comparing two hash values. If two hash values are equal, the ticket is a valid ticket. If not, the ticket is an invalid ticket. In this online money transfer system, bank administrators can sign and verify to achieve the goals of authentication and integrity of the system.

9. References

[1] Brian Gladman, Carl Ellison and Nicholas Bohm, "Digital Signatures, Certificates and Electronic Commerce" version 1, 1, June 8, 1999.

[2] David Youd , "An introduction to Digital Signatures" published 1996

[3] "Internet Banking" Comptroller of the Currency Administrator of National

[4] Mark Dermot Pyan, "One-way Secure Hash Functions", University of Brimingham, 2004.

[5] Pradosh Kumar Mohapatra, "Public Key Cryptography", ACM Student Magazine.

[6] Svetlin Nakov, "How Digital Signatures Work: Digitally Signing Messages", October 16,2003.

[7]http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html "Digital Signature Guidelines Tutorial"

[8]T. ElGamal (1985). "A public key cryptosystem and a signature scheme based on discrete logarithms".