

Secured Mail System using Asymmetric Cryptography – RSA and ElGamal Algorithm

Zarni Sann, May Thiri Win, San Thiri Aung

University of Computer Studies (Mandalay), Myanmar

Corresponding author's email id: zarnisann@gmail.com,

DOI: <http://doi.org/10.5281/zenodo.2917893>

Abstract

Mail messages are secure communication that transfers from one computer to another computer. In this system, user sends mail message to another user and, this message is stored in server by SMTP protocol. ElGamal encryption and RSA algorithm is made before storing mails to mail server. ElGamal decryption and RSA decryption is made after retrieving mails from mail server. When user receives a mail, server retrieves this mail served by POP protocol. This system is implemented to secure mail server system for local government's important mail messages. Implementation results of the system are secure patient records report for health department. Patient records must be secure for particular department. This system is based on locally own mail server mail client, and is implemented by using C# programming language and SQL Server to store mail messages.

Keywords: *Mail Server, Secure Communication, SMTP, POP, ElGamal algorithm, RSA algorithm*

INTRODUCTION

The system mainly consists of SMTP protocol and POP protocol for server and clients, and ElGamal algorithm for messages security. . ElGamal and RSA algorithm serves encryption and decryption of the mail messages.

Government's records must be secure for particular department. An email client or email program allows user to send and receive email by communicating with mail servers. A server works in the background, while the user usually interacts directly with a mail user. An email client, email

reader, is a computer program used to access and manage user's email. This system is based on locally own mail server and mail clients [6].

Emails are stored in the user's mailbox on the remote server until the user's email client requests them to be downloaded to the user's computer, or can otherwise access the user's mailbox on the possibly remote server. When user wishes to create and send an email, the email client will handle the task [7].

ElGamal algorithm is a type of cryptography. ElGamal algorithm is an asymmetric key cryptography, so it converts message strings to integers using "String to Integer conversion table". ElGamal's algorithm can convert original mail messages to cipher text, and can convert cipher text to plain text [2]. User can choose two algorithms to secure their messages. In this system, SMTP and POP are used in mail transferring and receiving, and ElGamal and RSA Cryptography is used for mail messages security.

RSA algorithm consist of three phases, phase one is key generation which is to be used as key to encrypt and decrypt data, second phase is encryption, where actual process of conversion of plaintext to

ciphertext is being carried out and third phase is decryption, where encrypted text is converted into plain text at other side. As a public key is used for encryption and is well known to everyone and with the help of public key, hacker can use brute force method to find private key which is used to decrypt message [5].

Mails are stored in server's database. Database is a store of information and can retrieve information. SQL database is used in this system. SQL server store patient records between clients as a database. E-mail and mail messages (such as Outlook Express or gmail) are used to sending and receiving mail over network or over the internet [7].

Organization of the paper

The paper is organized as follows: section 2 describes theory background of mail server architectures, and models. Section 3 explains ElGamal encryption and decryption and key generation for secure message. Section 3 also expresses RSA algorithm and its parameters. Section 4 presents briefly the proposed mail messages security using ElGamal and RSA algorithm as well as the step- by-step execution process of proposed architecture. Section 5 illustrates the implementation results with figures.

Finally, section 6 discusses on the conclusion, advantages, limitation and further extensions of the proposed system.

MAIL SERVER AND MAIL CLIENT

Mail server is a computer system that sends and receives electronic messages for a number of users in a certain management domain. The SMTP and POP protocols use between mail server and mail client. If a sender sends a mail messages to another one, this mail is stored into mail server machine. The process of mail sending and receiving using SMTP and POP is illustrated in **Figure 1** [3, 4].

Post Office Protocol (POP)

Using POP, user can download all emails to computer. POP supports simple download-and-delete requirements for access to remote mailboxes. Although most POP clients have an option to leave mail on server after download, mail clients using POP generally connect, retrieve all messages, store them on the user's PC as

new messages, delete them from the server, and then disconnect [4, 7].

Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is a standard for electronic mail (e-mail) transmission across networks. While electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically, use SMTP only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either the POP or the Internet Message Access Protocol (IMAP) or a proprietary system to access their mail box accounts on a mail server. [3].

The main function of text-based SMTP protocol is to "push" emails - it cannot "pull" them from servers which is why you also need POP. The "outgoing" mail server protocol helps servers communicate with each other and facilitate the delivery of the email message.

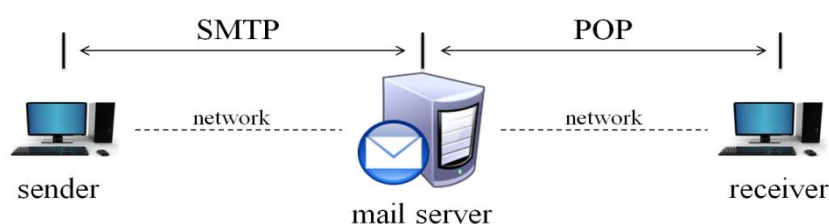


Fig. 1. Mail sending and receiving using SMTP and POP, and server

ASYMMETRIC CRYPTOGRAPHY

ElGamal encryption is used to encrypt the contents of a message so that it cannot be read by an unintended recipient [1, 2]. The algorithm is also able to decrypt the message, or make it readable again. The original, unencrypted message is readable to anyone who happens to intercept the message, so it is called the plaintext. The result of encrypting the plaintext is called a cipher text.

ElGamal algorithm

ElGamal algorithm is performed in three parts:

- Key generation for public keys and private keys
- Encryption for original plaintext message to receive cipher text, and
- Decryption for cipher text to generate original plaintext

ElGamal algorithm is illustrated in Figure 2. The key length of the ElGamal can range from 256-bit to arbitrarily long. A key length ranging from 1024 to 2048 bits are considered safe for the next 20 years. Private Key can range from 160 bit to 240 bit. ElGamal algorithm is an asymmetric key cryptography, so, it converts message

strings to digit using “String to digit conversion table”.

(a) Key Generation

Key Generation is the first stage of Elgamal algorithm. ElGamal describes the working steps of key generator as follows:

- Receiver generates an efficient description of a multiplicative cyclic group G of order q with generator g .
- Receiver chooses a random x from $\{1, \dots, q-1\}$.
- Receiver computes $h = gx$.
- Receiver publishes h , along with the description of G, q, g as her public key. Receiver retains x as private key which must be kept secret.

ElGamal proves and illustrates the key generator theory in the following algorithm: the first step in generating a public key is to choose a random large prime, called ‘ p ’, that is large enough to hide message. In key generation stage, prime number “ p ” should be used in large number than message keyword. [1, 2].

(b) Elgamal Encryption

Encryption is the second stage of Elgamal algorithm. Elgamal describes the working steps of encryption as follows:

- The encryption algorithm works as follows: to encrypt a message to receiver under her public key (G, q, g, h) ,
- Sender chooses a random y from $\{1, 2, \dots, q-1\}$, then calculates $c_1 = g^y$.
- Sender calculates the shared secret $s = h^y$.
- Sender converts his secret message m into an element m' of G .
- Sender calculates $c_2 = m' \times s$.
- Sender sends the ciphertext $(c_1, c_2) = (g^y, m' \times h^y) = (g^y, m')$ to receiver.

Note that one can easily find h^y if one knows m' . Therefore, a new y is generated for every message to improve security. For this reason, y is also called an ephemeral key. ElGamal proves and illustrates the encryption theory in the following algorithm: Message sender chooses a random integer 'r' for encryption and calculates ciphertexts using prime number 'p', random integer 'r' and plaintext 'P', and

generates pair of ciphertext for each block (C_1, C_2) . The following algorithm lines are the encryption stage in ElGamal [1, 2].

(c) Elgamal Decryption

Decryption is the third stage of Elgamal algorithm. Elgamal describes the working steps of decryption as follows:

- The decryption algorithm works as follows: to decrypt a ciphertext (c_1, c_2) with her private key x ,
- Receiver calculates the shared secret $s = c_1^x$
- and then computes $m' = c_2 \times s^{-1}$ which she then converts back into the plaintext message m , where s^{-1} is the inverse of S in the group G .

The decryption algorithm produces the intended message, since

$$c_2 \times s^{-1} = m' \times h^y \times (g^{xy})^{-1} = m' \times g^{xy} \times g^{-xy} = m'$$

The result of decryption process from the ElGamal algorithm and original incoming messages are the same. [1, 2]

RSA Operations

The RSA algorithm involves three steps:

- Key generation
- Encryption

- Decryption.

(a) Key Generation

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting message. Message encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated by the following way:

- It takes two random primes, p and q of approximately equal size such that $n = p \times q$.
- Compute $n = p \times q$, and $\phi(n) = (p-1)(q-1)$
- Choose an integer e , $1 < e < \phi(n)$, such that approaches, all equivalent in effect to factoring the $\gcd(e, \phi(n)) = 1$
- Compute d , $1 < d < \phi(n)$, such that $ed = 1 \pmod{\phi(n)}$
- The public key is (n, e) and the private key is (n, d) .

The value of p , q should also be kept secret. Both the sender and receiver must know the value of n . The sender knows the value of e and only the receiver knows the value of d . Thus this is a public key

encryption algorithm with a public key of $KU = \{e, n\}$ and a private key of $KR = \{d, n\}$ [1, 5].

(b) RSA Encryption

Sender wishes to send a message to receiver. Sender then computes the cipher text C : corresponding to $C = P^e \pmod{n}$. This can be done quickly using the method of exponentiation by squaring. Sender then transmits C to receiver. The letter will be used to refer the public key e , since the public key is used when encrypting a message.

(c) RSA Decryption

The receiver can recover P from C by using own private key exponent d by the following computation: $P = C^d \pmod{n}$. The letter d will be used to decrypt a message [1, 5].

SYSTEM DESIGN AND ARCHITECTURE

The constructed system can be divided into three main parts: the server computer with SQL database, one mail sender client and another one mail receiver client. The sender/receiver clients can be further divided into two sub sections: messages sending and message receiving.

If a sender sends a mail messages to another one, this mail is stored into mail server machine. ElGamal or RSA encryption is made before storing mails to mail server. ElGamal or RSA decryption is made before retrieving mails from mail server. This system contains a mail server and clients, using SMTP and POP, and ElGamal or RSA crypto algorithm for message security. ElGamal or RSA converts the mail messages as encrypted text and then again decrypted text. Mail

server stores mail messages until mail are not retrieved from receiver clients.

The process of system with two clients is shown in figure 2. This system is not allowed to view incoming mail before account login. The user must make login before account using. In this figure 3, patient record must enter for input data and system generate key $(e1, e2, p)$ for encrypting patients records report file for medical patient records.

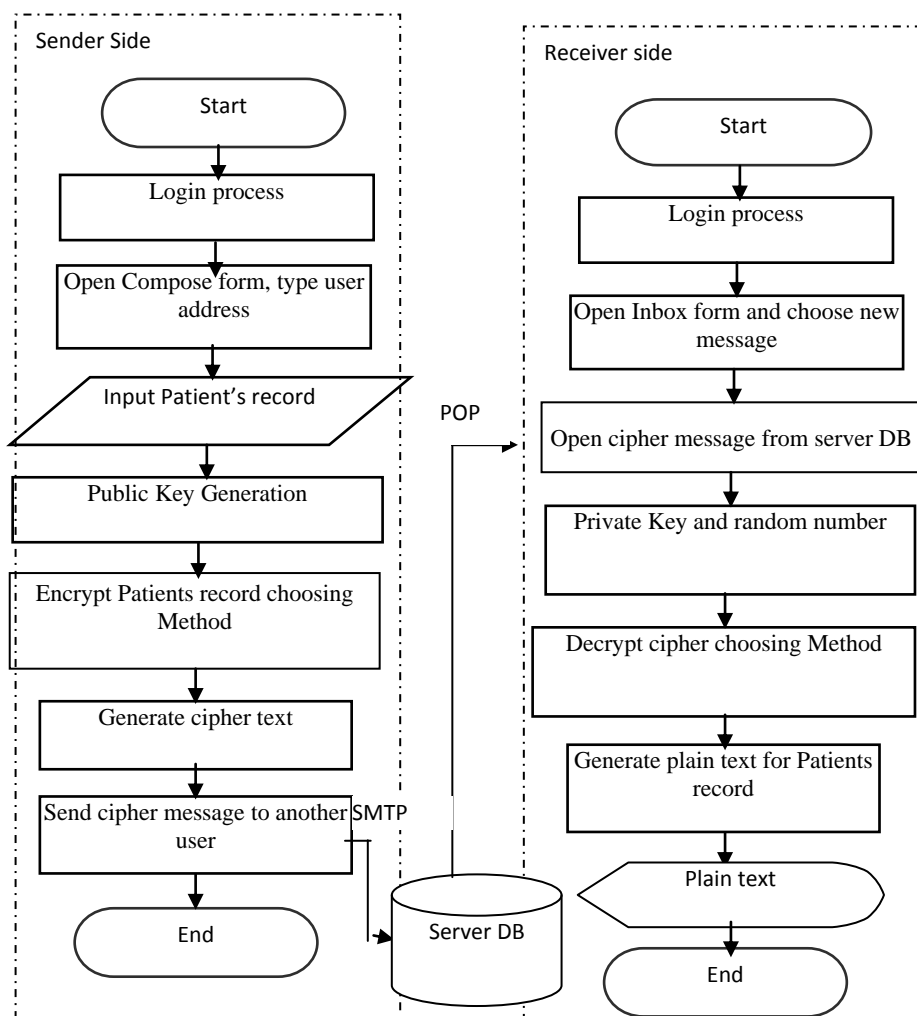


Fig. 2 System flow diagram

After encrypting patients' record, system display cipher text message and also sender client send cipher text message to another client. Server database stored this cipher message using SMTP protocol. If user want to know mail messages from server side, all message are displayed by cipher text. So receiver client retrieve this cipher text message using POP protocol. Receiver client generate prime number and random key and decrypt this cipher text using ElGamal or RSA decryption algorithm to obtain plain text.

IMPLEMENTATION RESULT

SQL database server is used in this system because SQL queries can be used to retrieve large amount of records from a database quickly and efficiently. The system has presented the design and implementation of own mail server system [7]. SMTP serves the work for sending

messages to mail server. POP serves the work for retrieving messages from mail server. ElGamal or RSA algorithm serves encryption and decryption of the mail messages.

Client users can send and retrieve mail and messages if their computers have connections with server computer. Connection means the local area network connection or wide area network connection. This network can be connected using network cable or wireless adapter. Figure 3 displays the login name and password for user Login in that is the address of @oms.com.

This system is implemented for security of messages on mail using ElGamal and RSA algorithms. It is developed by using C# Programming Language.

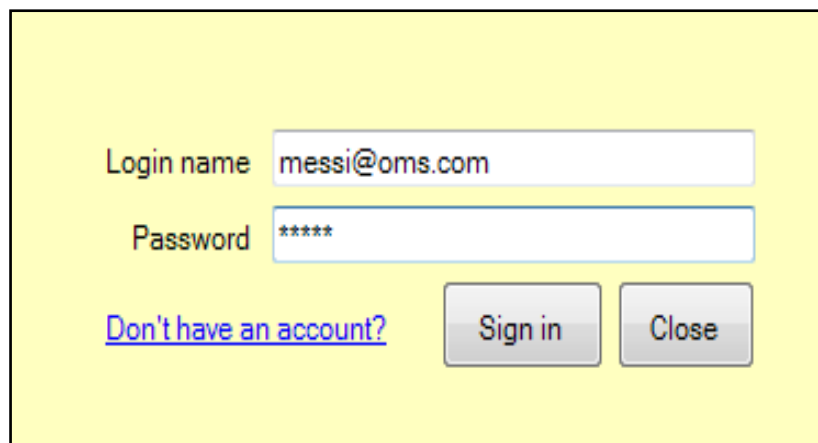
The image shows a user login form with a yellow background. It contains two input fields: 'Login name' with the text 'messi@oms.com' and 'Password' with masked characters '*****'. Below the password field is a blue underlined link that says 'Don't have an account?'. To the right of the link are two buttons: 'Sign in' and 'Close'.

Fig. 3 User login form

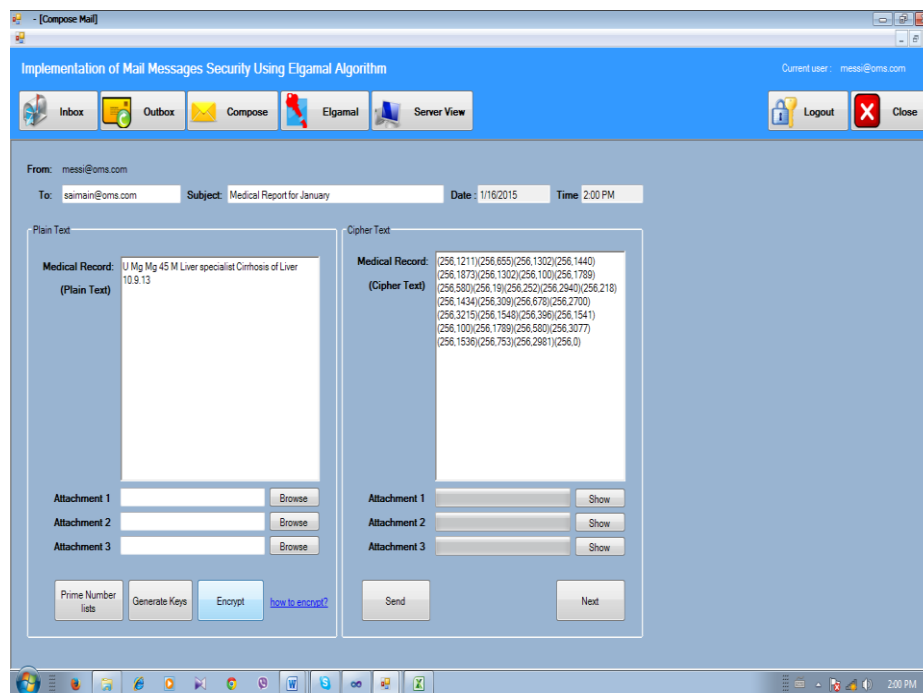


Fig. 4 Compose mail form for creating mail message and encryption process in sender side

In figure 4, message reaches in inbox of receiver side. If user want to view the select mail from read button. The system retrieves these cipher text mail message from server database. User can also see the date and time, sending address of incoming mail in figure 5.

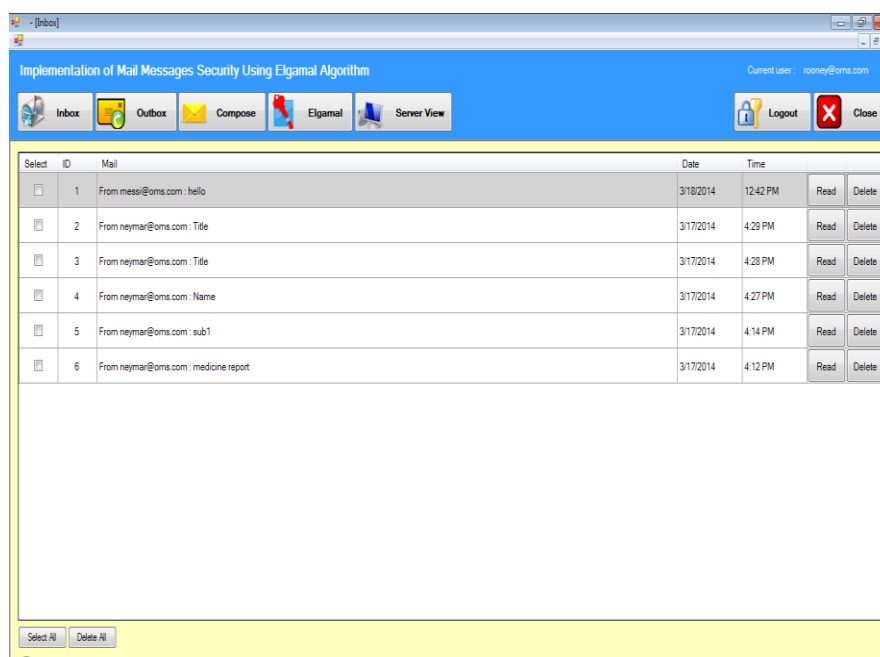


Fig. 5 Cipher text mail message in receiver's inbox form

In this figure, user creates new mail for medical record in message with attachment file for many records for patients in figure 6.

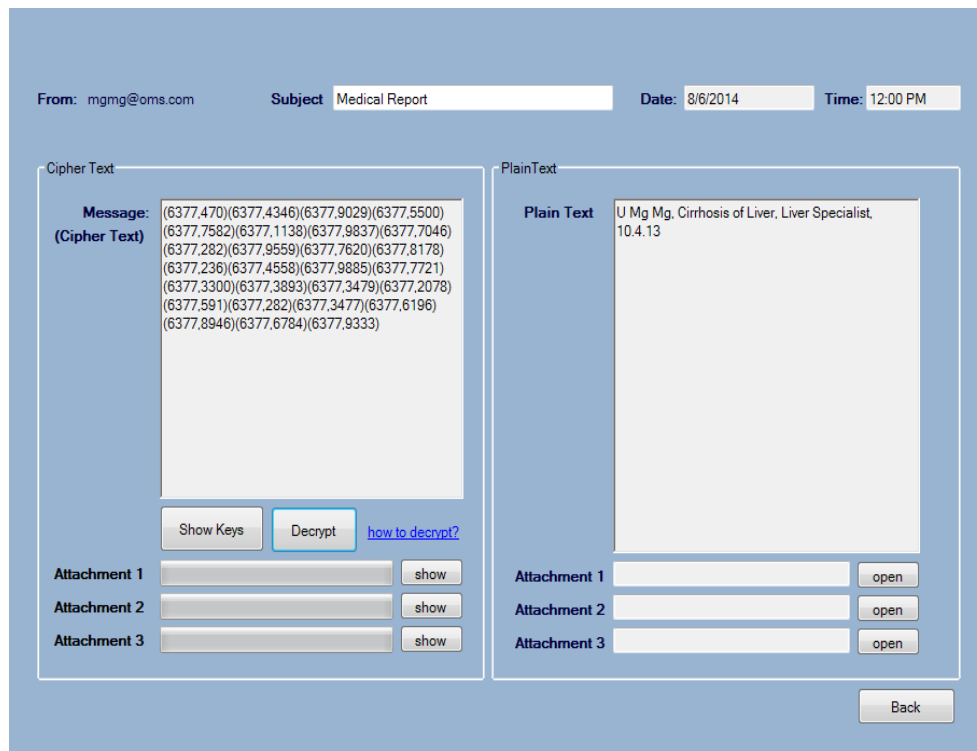


Fig. 6 Decrypted message in receiver side

This system can generate three attachment file and encrypt this files as shown in figure 7.

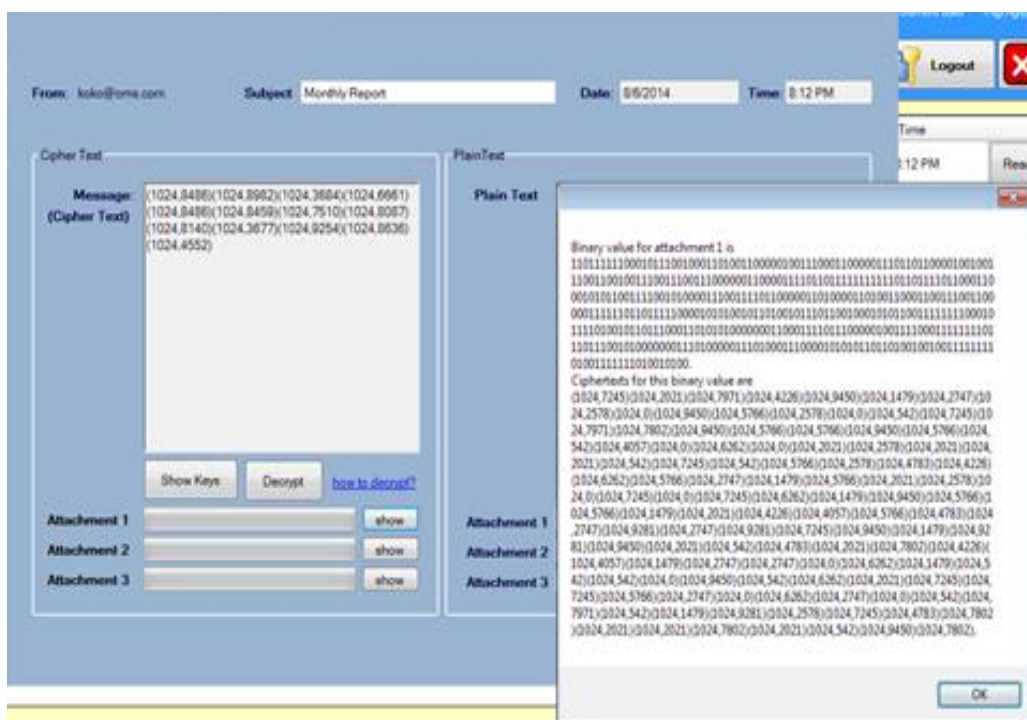


Fig. 7 Encrypted mail message with attachment file

In receiver side, user accepts attachment file for medical reports from receiver inbox. So uses decrypt button to open the original message. This system can decrypt three attachment files in figure 8.

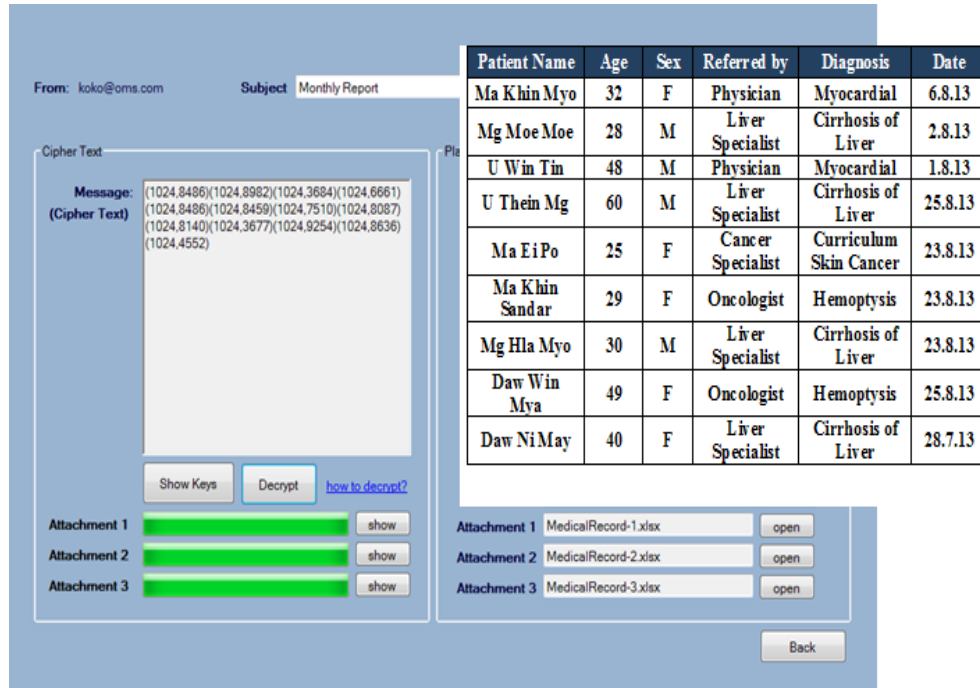


Fig. 8 Decrypted message with attachment file in receiver side

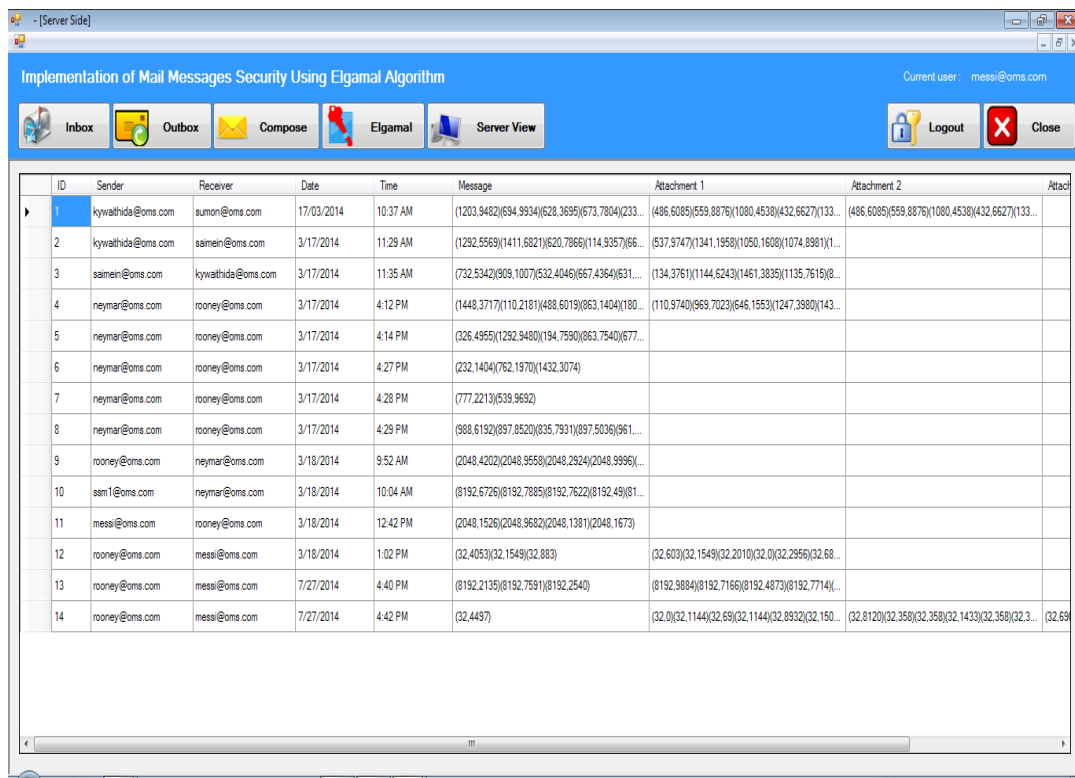


Fig. 9 Cipher text mail messages from server side

In mail server, there are incoming mail and outgoing mails for several clients. This mail server describes client ID for sender and receiver, sending date and time. In the server view, all messages (cipher text) are decrypted style with ElGamal and RSA security and specific attachment files also displayed with cipher text of decrypted style.

CONCLUSION

This system used ElGamal and RSA Cryptography for mail messages security. The system is implemented for the whole mail server process and cryptography is used for mail messages security. The effective of the system are: can make efficient and flexible mail services for user, can implement mail sending and receiving architecture.

Hence using cryptographic algorithm: RSA provides mail security solution in mail security system. It provides security services such as confidentiality, authentication, integrity and nonrepudiation. RSA encryption is faster than RSA decryption.

Mail server can store 64 bits (264 word counts) as maximum for cipher text values. So, server can store many cipher texts for each mail. The information of users and

mails are stored and protected by the mail server. It isn't necessary to wait until someone else gets around to adding new users. Not only the mail delivery is possessed quickly throughout the network, but also any mail coming in is receives immediately.

The limitation of the system is by using account extension (someone@oms.com). The account extension of this system is @oms. "oms" means "Own Mail Server". Other account extension types are not supported in this system such as someone@gmail.com, someone@fb.com and etc. Further extension of mail server is implementation of mail server using internet connections. However, it needs web page such as www.gmail.com. This system can extend the sender and receiver address security using another secure method.

REFERENCES

- I. Annapoorna Shetty, Shravya Shetty K, Krithika K, A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm, International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 5, October 2014

- II. Czeslaw Koscielny. A new approach to the Elgamal encryption scheme, Academy of Management of Legnica, Faculty of Computer Science, ul. Reymonta 21, 59–220 Legnica, Poland, Int. J. Appl. Math. Comput. Sci., 2004, Vol. 14, No. 2, 265–267
- III. J. Klensin, Simple Mail Transfer Protocol, RFC: 2821, Editor, AT&T Laboratories, Network Working Group, Request for Comments: 2821 Obsoletes: 821, 974, 1869 Updates, Category: Standards Track, April 2001
- IV. Jae-Young Kim and James Won-Ki Hong. Design and Implementation of a Web-based mail server management system, 1996. Algorithm, IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139
- V. M. Preetha, M. Nithya, A Study and Performance Analysis Of RSA Mustafa Dulegerler, M.Nusret Sarisakal. A secure e-mail application using the ElGamal algorithm, Istanbul University, Engineering Faculty, Computer Engineering Department, 34850, Turkey, 1998s.
- VI. Wei-Jaw Denga, Wen-Chin Chenb, Wen Peia. Own mail server implementation with client/server network architecture, 1997.

Cite this Article As

Zarni Sann, May Thiri Win, San Thiri Aung (2019). **Secured Mail System using Asymmetric Cryptography – RSA and ElGamal Algorithm** Journal of Networking, Computer Security and Engineering, 4(1), 46- 59

<http://doi.org/10.5281/zenodo.2917893>

AUTHORS' PROFILE

[1] Zarni Sann, Professor

Department: FCST

College: University of Computer Studies (Mandalay), Myanmar

Email Id: zarnisann@gmail.com

[2] May Thiri Win, Assistant Lecturer

Department: FCST

College: University of Computer Studies (Mandalay), Myanmar

Email Id: maythiriwin@gmail.com

[3] San Thiri Aung, Assistant Lecturer

Department: FCST

College: University of Computer Studies (Mandalay), Myanmar

Email Id: 3santhiriaung@gmail.com