OBJECT ORIENTED PARADIGM FOR IMPLEMENTING ELGAMAL ALGORITHM

Abikoye Oluwakemi C.
&
Nwokolo Ndidiamaka P.
Department of Computer Science, University of Ilorin, Ilorin, Nigeria

Abstract

The need of exchanging messages secretly over unsecure networks promoted the creation of cryptography to enable in the security of the messages sent over an unsecure network and also to enable only the authorized receivers to interpret the exchanged message. The main goal of the paper is to enable people who do not have the full knowledge of programming language to understand how the proposed system will work and also to enable programmers to implement the Elgamal algorithm using Object oriented approach. It also helps to prevent unauthorized access from interpreting the exchange messages. In the proposed system, Object oriented paradigm is designed to implement a particular public key cryptosystem called the Elgamal Cryptosystem is considered with the help of JAVA Programming language to be used over texts. Since the Elgamal cryptosystem was used in messages over a primitive root of a large prime; the proposed system showed how secure messages were sent over the network, and how the generations of public key was done in an encapsulated way.

Keywords: Cryptography, Elgamal algorithm, Cryptosystem, Object Oriented, Security

Introduction

Message encryption (Security) is a very crucial aspect in today's World, where computers and electronic media are used for transferring sensitive information like electronic mail, bank accounts, electronic cash, username and password, personal document and so on. These computers and electronic media are vulnerable to security threat (which would be interruption, privacy-breach, integrity, and authentication) and security attacks (this attack are classified into passive and active attack) (Stallings, 2011). Today, the protection against misuse, manipulation and attackers of messages being sent on-line has been considered as the basic challenge of this new era. Cryptography is one of the steps taken in order to secure data and messages that are being sent through these computers and electronic media(s) via the internet.

Cryptography is the science and study of Secret (crypto-)-Writing (-graphy). A cipher is a secret method of writing, whereby plaintext (or cleartext) is transformed into ciphertext (sometimes called a cryptogram). The process of transforming plaintext into ciphertext is called encipherment or encryption; the reverse process of transforming ciphertext into plaintext is called decipherment or decryption (Denning, 1982). It can also be the study of mathematical techniques related to aspects of information security to encrypt and decrypt data (Mark Adler and Jean-Loup Gailly, 2004). For cryptography to be an effective way of securing data it must be able to provide the following services such as confidentiality, data integrity, availability, entity authentication, non-repudiation and access control (Stallings, 2011).

In most of information been sent on the Internet, hackers have found it easier to attack user's information on a network due to the limitation of encryption and decryption system. User's documents are being hijacked by attackers whose intention is to defraud the recipient's documents. According to Hamdan et.al., (2010), with the rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the internet, also the Internet allows for wide distribution of digital media data, so this becomes much easier to edit, modify and duplicate digital information. In symmetric algorithm, the keys are not use for a more computationally intensive and therefore are mostly use for securing short text messages (Sudhir et.al, 2012). In order to conquer this problem an asymmetric algorithm is use to solve the problem of symmetric algorithm where two keys (public key and private key) are needed for the encrypting and decrypting of messages. Based on this problem stated above there is need of developing a message encryption and decryption system that would use a more advance algorithm called an asymmetric (Elgamal) algorithm.

Objectives of the Study

The objectives of this paper work are to:

i. review existing literature on cryptography;
ii. design a message security model using Elgamal algorithm; and
iii. design an object oriented paradigms for implementing the model.

Literature Review

Overview of Cryptography

Message security is mostly done by a means known as cryptography. Cryptography has been defined by many Authors. According to Denning (1982), cryptography is the science and study of secret writing. Santosh (2010), define cryptography as the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data again authentication. Padmavathi and Ranjitha (2013), define cryptography is an effective way for protecting sensitive information, it is a method for storing and transmitting data in form that only those that it is intended for read and process.

Amoghand Rajballav (2007) also define cryptography as the science or art of encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form. As the field of cryptography became advanced; cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances. The field of cryptography also deals with the techniques for conveying information securely. The goal of cryptography is to allow the intended recipients of a message to receive the message securely. Cryptography tries to

prevent the eavesdroppers from understanding the message. Cryptography is majorly of two forms, they are symmetric and asymmetric cryptography.

Symmetric Cryptography

In symmetric cryptography, the process of encryption and decryption is done using the same key. This form of cryptography is also called conventional encryption. Symmetric encryption transforms plaintext into ciphertext using a secret key and an encryption algorithm, in decrypting the ciphertext the same key is use and a decryption algorithm, after which the plaintext is then recovered from the ciphertext (Stallings, 2011).

A conventional encryption model can be illustrated as assigning Xp to represent the plaintext message to be transmitted by the sender. The parties involved select an encryption algorithm represented by E. The parties agree upon the secret key represented by K. The secret is distributed in a secure manner represented by SC. Conventional encryption's effectiveness rests on keeping the key secret. Keeping the key secret rests in a large on key distribution methods. When E processes Xp and K, Xc is derived. Xc represents the cipher text output, which will be decrypted by the recipient. Upon receipt of Xc, the recipient uses a decryption algorithm represented by D to process Xc and K
back to Xp.

Symmetric cryptography has some merit over the other form of cryptography. Some of which are:

- Symmetric cryptography is efficient; it takes less time to encrypt a message.
- The key use in symmetric cryptography is relatively small.
- Symmetric cryptography can be composed to produce stronger ciphers. Simple transformations which are easy to analyze, can be used to construct strong product ciphers.

While it demerits are:

- The key in use must be shared only between two users.
- The management of the key in a large network is as many as ((n(n-1))/2) making it tedious to manage the key pairing process.

Examples of symmetric cryptography algorithm are Data Encryption Scheme (DES), Advance Encryption Scheme (AES), Triple DES, etc.

Asymmetric Cryptography

Asymmetric cryptography is also known as Public-Key Algorithms. In this form of cryptography the key used in encrypting the message is different from the key used in decrypting the message. The encryption key, known as the Public key is used to encrypt a message, but the message can only be decoded by the person that has the decryption key, known as the private key. This type of encryption has a number of advantages over

traditional symmetric encryption. It means that the recipient can make their public key widely available- anyone wanting to send them a message uses the algorithm and the recipient's public key to do so. An eavesdropper may have both the algorithm and the public key, but will still not be able to decrypt the message. Only the recipient, with the private key can decrypt the message.

An advantage of public-key algorithm is that they are more computationally intensive than symmetric algorithms, and therefore encryption and decryption take longer. This may not be significant for a short text message, but certainly is for bulk data encryption. Beside, from the advantage mentioned above, asymmetric cryptography still has a lot of merits over symmetric. Some of which are:

- The primary advantage of public-key cryptography is increased in security and convenience. The Private keys are never transmitted or revealed to anyone, unlike the secret-key system, where the secret keys must be transmitted (either manually or through a communication channel), and there may be a chance that an enemy can discover the secret keys during their transmission.
- Another major advantage of public-key systems is that they can provide a method for digital signatures.

There is no method that has merit without demerit. Some of the disadvantages of using public-key cryptography are:

- Public-key cryptography for encryption has limited speed; there are popular secret-key encryption methods that are significantly faster than any currently available public-key encryption method. Nevertheless, public-key cryptography can be used with secret-key cryptography to get the best of both worlds.
- Public-key cryptography may be vulnerable to impersonation, however, even if users' private keys are not available. A successful attack on a certification authority will allow an adversary to impersonate whomever the adversary chooses to by using a public-key certificate from the compromised authority to bind a key of the adversary's choice to the name of another user.

However, public-key cryptography is not meant to replace secret-key cryptography, but rather to supplement it, to make it more secure. The first use of public-key techniques was for secure key exchange in an otherwise secret-key system; this is still one of its primary functions. Secret-key cryptography remains extremely important and it is still in use these days. Examples of asymmetric cryptography algorithm are Rivest Shamir Adleman (RSA), Diffie-Hellman Key Exchange Algorithm, Elgamal Public Key System, etc.

The RSA Algorithm

The RSA cryptosystem is one of the public-key cryptography, named after its inventors R. Rivest, A. Shamir, and L. Adleman, and it is the most widely used public key Cryptosystem in the world. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization.

Diffie-Hellman Key Exchange Algorithm

Diffie and Hellman(1976), published the first public key based algorithm, which was designed to provide a means to exchange securely a key *K* over a public network. That key *K* can later be used as a session key. However this algorithm applies only to the exchange of keys.

Elliptic Curve Cryptography

Public key cryptography systems are usually based on the assumption that a particular mathematical operation is easy to do, but difficult to undo unless some particular secret is known. This particular secret serves as the secret key. A recent development in this field is the so-called Elliptic Curve Cryptography. Elliptic Curve Cryptography works with point on a curve. The security of this type of public key cryptography depends on the elliptic curve discrete logarithm problem. Elliptic curve cryptography was invented by Neil Koblitz in 1987 and by Victor Miller in 1986. The principles of elliptic curve cryptography can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or EIGamal. Although no general patent on elliptic curve cryptography appears to exist, there are several patents that may be relevant depending on the implementation. The main advantage of elliptic curve cryptography is that the keys can be much smaller. Recommended key sizes are in the order of 160 bits rather than 1024 bits for RSA.

Elgamal Public Key System

The ElGamal cryptographic algorithm is a public key system like the Diffie-Hellman system. It is mainly used to establish common keys and to encrypt message. The EIGamal cryptographic algorithm is comparable to the Diffie-Hellman system. Although the inventor, TaherElgamal, did not apply for a patent on his invention, the owners of the Diffie-Hellman patent felt this system was covered by their patent. For no apparent reason everyone calls this the IElGamal" system although Mr. Elgamal's last name does• not have a capital letter 'G'.

Generating the ElGamal Public Key

As with Diffie-Hellman(1976), Amaka and Shalom have a (publicly known) prime number p and a generator g. Amaka chooses a random number a and computes $A = g^a \bmod p$. Shalom does the same and computes B = gb mod p. Amaka's public key is A and her private key is a. Similarly, Shalom's public key is B and his private key is b.

Encrypting and Decrypting Messages

If Shalom now wants to send a message m to Amaka, she randomly picks a number k, which is smaller than p. He then computes:

$C1 = m*k \bmod p$
And send C1 to Alice. Alice can use this to reconstruct the message m by Computing
$C2 = k^{-1}*C1 \bmod p$

Review of Related Studies

Ambalika and Sunil (2014) proposed an Object Oriented Modeling of DSA for Authentication of Student in E-Learning. In their paper they said that E-Learning is the interactive transfer of knowledge via an intranet or the internet. Due to use of internet as electronic communication media there are several types of risks & threats that may hamper security of E-learning environment. At the time of online submission of filling up form during any course registration by student, the authenticity and integrity of the information can be ensured using digital signature. To enhance the security level of the information the Digital Signature Algorithm (DSA) can be used to generate digital signature which will be an industry standard algorithm using public key cryptography for security of various electronic systems like E-Governance, E-Banking, E- Commerce etc. In their paper, authors have applied DSA algorithm to achieve optimal resource allocation, faster information and enhanced security for authentication of information in E-Learning during submission of ICT (Information and Communication Technology) based filled up course registration form in Object Oriented paradigm.

Hayder and Irtifaa (2014), develop a system which can encrypt and decrypt Image in a modify way using an ElGamal cryptosystem in MATLAB. The need of exchanging messages and images secretly over unsecure networks promoted the creation of cryptosystems to enable receivers to interpret the exchanged information. In their paper, they use a particular public key cryptosystem called the ElGamal Cryptosystem with MATLAB to implement the program to be used over the Images. Their work shows a modification of the cryptosystem by applying it over gray and color images by transforming an image into its corresponding matrix using MATLAB Program, then applying the encryption and decryption algorithms over it. Actually, this modification gives one of the best image encryptions that have been used since the encryption procedure over any image goes smoothly and transfers the original image to completely undefined image which makes this cryptosystem to really secure and successful encrypt the image. As well as, the decryption procedure of the encrypted image works very well since it transfers undefined image to its original.

Obaida (2013), proposed a new approach for complex encrypting and decryption data. In his research, he combined public key infrastructure and RC6 algorithm. RC6 is used to generate private key based on secret value from public key infrastructure. Plaint-text 1024-bit size divided to 2 blocks. One of this block used as key after performed

confusion and diffusion operation using R6C algorithm. The key is then inserted inside the cipher data based on the private position. The same process used for encryption is also used to decrypt data. The algorithm proposed by Obaida is very secure and possesses average key unlike the Advanced Encryption Scheme (AES). But this algorithm is majorly based on the symmetric key cryptography technique.

Anwar and Riyazuddin (2011), design a "Transparent Data Encryption- Solution for Security of Database Contents". The study deals with ways to create Master Key, creation of certificate protected by the master key, creation of database master key and protection by the certificate and ways to set the database to use encryption in Microsoft SQL Server 2008. The purpose of their study is aimed at dealing with the most critical threats to which database is vulnerable. The transparent data encryption shields database up to considerable extent against threats and prevent intruders to have access to confidential database, reduce the cost of managing user and facilitate privacy managements. This technology allows encryption of databases on hard disks and on any backup media.

They also made use of database encryption key (DEK), which is stored in the database boot record for availability during recovery. It is an asymmetric key secured by using a certificate stored in the master database and Microsoft SQL Server 2008 is use to implement and encrypt database content. The limitation of this research is that the transparent data protection does not provide encryption across communication channels. It also need regularly backing up of the certificate and the private key associated with the certificate.

Yonglin, Azzedine and Lynda (2011), presents the principle of selective encryption with a propose of probabilistically selective encryption algorithm. The algorithm was based on symmetric key by making use of probabilistic methodology and stochastic algorithm, in the process of message encryption, a sender includes proper uncertainty, so that the decryption of the ciphertext is done by only entrusted receiver and other unauthorized nodes have no information of the broadcasted messages on the whole.

Myungsun ,Jihye, and Jung(2010), designed a system that compress multiple ciphertexts using elgamal encryption schemes. In their work they deal with the problem of how to squeeze multiple ciphertexts without losing original message information. To do so, they formalize the notion of decomposability for public-key encryption and investigate why adding decomposability is challenging. They construct an ElGamal encryption scheme over extension fields, and show that it supports the efficient decomposition. They then analyze security of their scheme under the standard DDH assumption, and evaluate the performance of the construction.

Their limitation is that they have the problem of inefficient scheme in the compression of the image in not losing it quality.

Methodology

Elgamal Public Key System

The ElGamal cryptography algorithm is a public key system like the Diffie-Hellman system. It is mainly used to establish common keys and to encrypt message. The Elgamal algorithm which uses Diffe-Hellman theory was generated in 1976. The Elgamal algorithm works on discrete-logarithm. The Elgamal algorithm is composed of three sub phases:

a. key generation algorithm;
b. encryption algorithm; and
c. decryption algorithm.

The Elgamal algorithm makes use of the following variables:
a = generator key (a must be between 1 and p-1)
x^a = Amaka's private key ($1 < x < p-2$)
x^b = Shalom's private key ($1 < x < p-2$)
p = prime number (chose a larger prime number).
m = message to be encrypted $[0 < m < p-1]$.
The public keys are calculated for both users as follows:
$pub_a = a^{xa} \bmod p$ (Amaka's public key)
$pub_b = a^{xb} \bmod p$ (Shalom's public key)
Let assume that the sender wants to encrypt a message m and send the encrypted message to the receiver. The following steps are to be taken;

1. both users agreed on the key generator a ($1 < a < p-1$) and also choses their private keys which is unique to them x^a and x^b($1 < x < p-2$);
2. both users also calculate their public key:
   i. $pub_a = a^{xa} \bmod p$
   ii. $pub_b = a^{xb} \bmod p$;
3. both user calculate the common key:
   i. $k_a = pub_b{}^{xa} \bmod p$
   ii. $k_b = pub_a{}^{xb} \bmod p$
4. the sender encrypt the message:

$C_1 = m * k \bmod p$ (C_1 = encrypted message(cipher))

5. the receiver decrypt the message:

$C_2 = k^{-1} * C_1 \bmod p$ (C_2 = decrypted message.) k^{-1} is calculated using the modular inverse. If $C_2 = m$ accept, otherwise reject.

The mathematical expression of the Elgamal public key system is shown below:
The proposed system is designed with Elgamal algorithm which uses Diffe-Hellman theory which was generated in 1976. The Elgamal algorithm works on discrete-logarithm.

Formula: $a^x \bmod p$

Key Generation:

Where a is a generator key (a must be between 1 and p-1)
x is the private key ($1 < x < p-2$)
p is a prime number (chose a larger prime number).
m is the message to be encrypted $[0 < m < p-1]$
Encrypting a message.i.e. sending a message from Alice to Bob.
Let $p = 139$, $x_a = 12$ (Alice private key), $x_b = 15$ (Bob private key), $a = 3$, $m = 100$.

To calculate the public key for Amaka

$pub_a = a^{xa} \bmod p$
$=3^{12} \bmod 139$
$=531441 / 139 = 3823$
$=531441 - (139*3823)$
$=44$

To calculate the public key for Shalom

$pub_b = a^{xb} \bmod p$
$=3^{15} \bmod 139$
$=14348907 / 139 =103229$
$=14348907 – (139*103229)$
$=14348907-14348831$
$=76$

To Get the Common Key Between Amaka and Shalom Use for Encryption and Decryption of their Messages.
For Amaka
$k_a = pub_b{}^{xa} \bmod p$
$=76^{12} \bmod 139$
$= 37133262473195501387776 / 139 = 267145773188456844516$
$=37133262473195501387776 – (139*267145773188456844516)$
$=37133262473195501387776 – 37133262473195501387724$
$=52.$

For Shalom

$k_b = pub_a^{xb} \bmod p$
$=44^{15} \bmod 139$
$=448528606872902211888742 4 / 139 = 32268245098769943301348$
$=448528606872902211888742 4 – (139*32268245098769943301348)$
$=448528606872902211888742 4 – 448528606872902211888737 2$
$=52$

To Encrypt a Message:

$C_1 = m * k \bmod p$
$= 100*52 \bmod 139$
$=5200 / 139 = 37.41$
$=5200 – (37*139)$
$= 57$

To Decrypt a Message:

$C_2 = k^{-1} * C_1 \bmod 139$ (k^{-1} is calculated using the modular inverse).
$k^{-1} = \bmod 139$
$k.* = 1 \bmod 139$
$x = (1/k) \bmod 139$
prime number = k(multiple) + remainder
$139 = 52(2) + 35$
$52 = 35(1) + 17$
$35 = 17(2) + 1$
Re-arranging to get an equation
$139 + 52(-2) = 35 \ldots 1$
$52 + 35(-1) = 17 \ldots 2$
$35 + 17(-2) = 1 \ldots 3$
Start from equation 3
$35 + 17(-2) = 1$
$35 + (52+35(-1))\ (-2) = 1$
$35 + 52(-2) + 35(-2) = 1$
$35 + 35(-2) + 52(-2) = 1$
$35(1+2) + 52(-2) = 1$
$35(3) + 52(-2) = 1$
$(139 + 52(-2))(3) = 1$
$139(3) + 52(-6) + 52(-2) = 1$
$139(3) + 52(-6 + (-2)) = 1$
$139(3) + 52(-8) = 1 \bmod 139$
$0 + 52(139-8) = 1 \bmod 139$
$0 + 52(131) = I \bmod 139$
$131 = (1/52) \bmod 139$
The inverse modular for k^{-1} (52^{-1}) = 131

To Decrypt

$C2 = k^{-1}\ c1 \bmod 139$
$= 131 * 57 \bmod 139$
$= 7467 / 139 = 53.71\ldots$
$= 7467 - (139*53)$
$= 7467 - 7367$
$= 100$

Elgamal Encryption and Decryption Algorithm

Encryption Algorithm

- Obtain the public key from the receiver B in order to get the common key.
- Choose an integer xa such that : $1 < xa < p-2$
- Represent the plaintext as an integer m where $0 < m < p-1$
- Compute (k) as follows: $k= a^{xa} \bmod p$
- Compute (C1) as follows: $C1 = (k * m) \bmod p$
- Send C1 to receiver B.

Decryption Algorithm

- Obtain the ciphertext (C1) from sender A.
- Compute (C2) as follows: $C2 = k\text{-}1*C1 \bmod p$
- And recover the plaintext, m

RESULTS AND DISCUSSION

Object Oriented Paradigm

Unified Modeling Language (**UML**) approach is used as the object oriented paradigm for the design of the Elgamal algorithm. An object contains both data and methods that control the data. The data represents the state of the object. The **Unified Modeling Language** (**UML**) is made up of different types but this paper discusses on three major types.

1. Use case diagram.
2. Sequence diagram.
3. Class diagram.

Use case diagram

Use case represents a set of actions performed by a system for a specific goal. Use case diagrams are also a set of use cases, actors and their relationships. They represent the use case view of a system. A use case represents a particular functionality of a system.http://www.tutorialspoint.com/uml

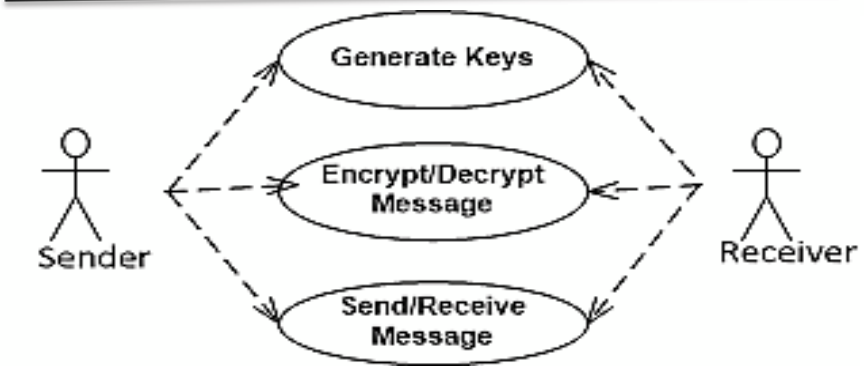

Figure 1: Use case diagram

Sequence diagram

A sequence diagram is an interaction diagram, it shows how sequence of messages flows from one object to another. Interaction among the components of a system is very important from implementation and execution perspective. So Sequence diagram is used to visualize the sequence of calls in a system to perform a specific functionality.

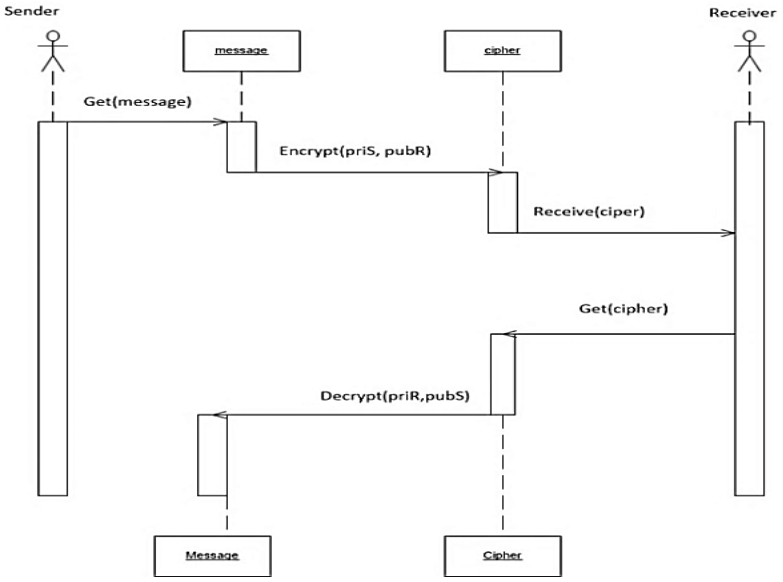

Figure 2: Sequence diagram

Class Diagram

Class diagrams are the most common diagrams used in UML. Class diagram consists of classes, interfaces, associations and collaboration. Class diagrams basically represent the object oriented view of a system which is static in nature.Class diagrams are made

up of attributes and methods. In this paper the attributes are those above the line in a section and the methods are those below the line in the section.

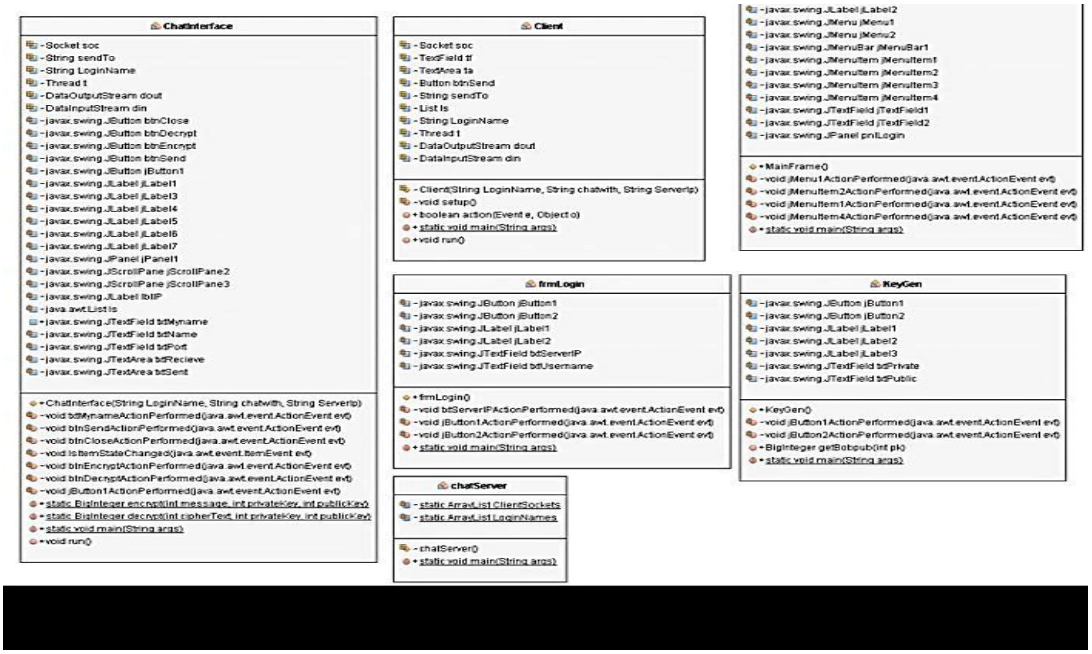

Figure 3: Class diagram

The use case diagram, the sequence diagram and the class diagram explain fully well how the Elgamal algorithm works. Using Elgamal algorithm an asymmetric type of cryptography to secure messages, the keys must be generated first after which the encryption processes is done. During the process of encryption the sender must supply its own private key which is only know to the him or her and the receiver public key which is mostly know to the public and the send the encrypted message to the intended receiver. The receiver receives the message and starts the decryption process. To decrypt the message the receiver will supply his or her private keys and the sender public keys, so has to understand the content of the message sent to him or her. Cryptography is very useful in message encryption, though not 100% efficient but it is efficient when it is being able to keep the confidentiality, integrity and provide the message in time (i.e. availability of the message). The purpose of the encryption and decryption process is to achieve the following:

i to secure message on the network and also the network itself, data, files etc.
ii to secure message communicated from one system to another on the network (internet).
iii to also enable the establishment of a secure channel for key sharing and encrypting & decrypting of messages.
iv to also prevent the eavesdroppers from understanding the message.
v. to allow the intended recipients of a message to receive the message securely.

Limitation

This paper works does not include the features for encrypting and decrypting scanned documents and images. The disadvantages of Elgamal algorithm include slow in speed, message expansion by a factor of two during encryption, semantically insecure and require randomness during operation (Adewole. et. al, 2014).

Conclusion

The need to develop a system that would assist the control of message security cannot be over emphasized. However, this study helps to solve some of the problem associated with current system by introducing the use of public and private key. Elgamal system is a public key cryptosystem that is based on discrete logarithm problem. In this paper, a message securitymodel was developed using Elgamal algorithm in the form of object oriented paradigm. Elgamal algorithm used both public and private key, hence, it is asymmetric encryption algorithm.

Recommendations

The symmetric cryptography system has been reviewed and new system software that will aid security control has been developed using object oriented paradigm for implementing Elgamal algorithm. The securing of vital information is essentially important. This paper works also show how to paper is recommended for exchange messages over the internet.Further research could be done in by combining both the symmetric and asymmetric cryptography in order to improve the efficiency and application of the system for securing data and information.

References

Ambalika Ghosh, Sunil Karforma. (2014). Object Oriented Modeling Of Dsa For Authentication Of Student In E-Learning . India:

Amogh M & Rajballav D. (2007). Data Encryption And Decryption By Using Hill Cipher Technique And Self Repetitive Matrix. Rourkela.

Anwar P.A & Riyazuddin Q. (2011). Transparent Data Encryption- Solution For Security Of Database Contents. *International Journal Of Advance Computer Science And Application*, 25-28.

Babatunde A.O., Adewole K.S.,Abdulraheem & Oniyide S.A. (2014). A Network-Based Key Exchange Crytptosystem Using Elgamal Algorithm. Arican Journal Of Computing & Ict , 45-52.

Dorothy, E. (1982). Cryptography And Data Security. United State Of America.: Addison-Wesley Publishing Comany, Inc.

Haydeen R.H & Irtifaa A.N. (2014). Image Encryption And Decryption In A Modification of Elgamal Cryptosystem In Mathlab. *International Journal Of Sciences: Basic And Applied Research*, 141-147.

Knudsen, J. B. (1998). Java Cryptography. O'reilly.