

A Network-based Key Exchange Cryptosystem Using Elgamal Algorithm

¹A.O. Babatunde, K.S. Adewole, ²M Abdulraheem & ³S.A. Oniyide

¹Department of Computer Science, University of Ilorin, Ilorin

²Computer Services and Information Technology Directorate, University of Ilorin, Ilorin

^{1,2}{adewole.ks, babatunde.ao, muyideen@unilorin.edu.ng}

ABSTRACT

A cryptosystem describes the system where two or more individuals communicate in a secret manner over a public channel. The contents of information shared on a public network need to be protected against unauthorized access using a more secured technique of encryption and decryption. A cipher is the heart of a cryptosystem, which specifies the policy for encryption and decryption. The encryption policy takes the plaintext and a predetermined key, and produces a ciphertext which hides the true meaning of the original plaintext. The decryption policy takes another key, which may be different from the encryption key, and recovers the plaintext from the ciphertext. In this paper, a cryptosystem is developed using Elgamal algorithm for key exchange purpose during information sharing on a public network. The proposed system provides a secure platform for encrypting and decrypting user's key. This key could be used by a symmetric algorithm for file encryption and decryption. The system is found capable of securing user's key from illegal access by an unauthorized person.

Keywords: Cryptosystem, Cipher, Elgamal, Encryption, Decryption

African Journal of Computing & ICT Reference Format:

A.O. Babatunde, K.S. Adewole, M Abdulraheem & S.A. Oniyide (2014). A Network-based Key Exchange Cryptosystem Using Elgamal Algorithm. Afr J. of Comp & ICTs. Vol 7, No. 2. Pp45-52.

1. INTRODUCTION

Computer has been primarily used by university researchers in some years back majorly for information transfer among academics and organizations for resource sharing purpose. These resources include printers and scanner. At this time, security was not on the priority, and such shared information and resources do not pose any security risk to sender or receiver. Nowadays, the use of computer has gone beyond their early intentions. Today's information technology security environment consists of highly interactive and very powerful computing devices and interconnected systems of systems across global networks to share resources among individuals [1].

This has led to the need for tight security to data and information as they are transported across public networks. The security of communications and commerce in a digital age relies on the modern incarnation of the ancient art of codes and ciphers. Underlying the birth of modern cryptography is a great deal of fascinating mathematics, some of which has been developed for cryptographic applications, but much of which is taken from the classical mathematical rules [4]. Cryptography is the science concerned with linguistic and mathematical techniques for securing information [6].

Cryptography has been concerned solely with encryption which involved converting information from its normal, comprehensible form into an incomprehensible format, thus rendering it useless without secret knowledge [2]. Cryptography is used in application represent in technological advanced societies; examples include the security of email, ATM cards, computer passwords and electronic commerce which all depend on cryptography. Indeed, the principal goal in the design of any cryptographic system is security [7].

A cryptosystem describes a way for two or more parties to communicate in secret over a public channel. The content of the communication, which may be human language or anything else, is called the plaintext. The heart of a cryptosystem is a cipher, which specifies rules for encryption and decryption. The encryption rule takes the plaintext and a pre-determined key, and produces a ciphertext which hides the content of the original plaintext. The decryption rule takes another key, possibly different from the encryption key, and recovers the plaintext from the ciphertext. There are two basic types of cryptosystems: symmetric key (private key) systems and public key (asymmetric) systems[4][3]. Public key systems are much slower than symmetric systems, but symmetric systems require key agreement through an existing secure channel, hence, the two systems can be combined.

Symmetric systems include Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Skipjack [3]. In cryptosystem, there is an assumption that two people called Yetunde and Matthew attempt to share a secret key that Ibitoye does not possess. Yetunde used the secret key to encrypt her message and Matthew used the same secret key to decrypt the message. Meanwhile, Ibitoye could not decrypt the message since he did not have any idea of what the secret key is. A disadvantage of this cryptosystem as pointed out by [4] is that Yetunde and Matthew need to exchange the secret key. To overcome this challenge of key exchange, a public key cryptography was introduced. In this system, Yetunde has two keys, a public key and a private key. The public key possessed by Yetunde is published and anyone including Matthew can use this key to encrypt message and send this encrypted information to Yetunde. In this cryptosystem, Yetunde is the only authorized user who can decrypt the message since she alone knows the private key. ElGamal algorithm is asymmetric algorithm since two different keys are used during encryption and decryption process.

1.1 Diffie-Hellman Key Exchange

Diffie-Hellman is a name derived from the inventors of public key encryption system. These scientists are called Whitfield Diffie and Martin Hellman who published a paper titled "New Directions in Cryptography" in 1976[4]. Diffie-Hellman method for key exchange is based on the assumption that the discrete logarithm problem (DLP) is difficult to solve. In their article, Diffie and Hellman also defined a variety of cryptanalytic attacks and introduced the important concepts of digital signatures and one-way authentication. ElGamal is a continuation of Diffie-Hellman key exchange algorithm [5][11].

The Diffie-Hellman key exchange algorithm solves the problem that may arise during key exchange through an insecure channel. Yetunde and Matthew attempt to share a secret key for use in a symmetric cipher through an insecure communication channel. Assuming Ibitoye is observing every piece of information they exchange. There is a need for Yetunde and Matthew to choose a better approach to exchange the secret key without making it known to Ibitoye. This dilemma can be solved using Diffie-Hellman approach. In this approach, Yetunde and Matthew first agreed a large prime p and a nonzero integer g modulo p . Yetunde and Matthew make the values of p and g public so that anybody can access them. This could be through a web page or other public channels. Since p and g are published, Ibitoye knows the two values. Let us assume that Yetunde and Matthew choose g such that its order in F_p^* is a large prime.

Yetunde picks a secret integer a that she does not reveal to anyone, while at the same time Matthew picks an integer b that he keeps secret. Yetunde and Matthew use their secret integers to compute

$$A \equiv g^a \pmod{p} \quad (1.1)$$

$$B \equiv g^b \pmod{p} \quad (1.2)$$

The next stage is for them to exchange their computed values. Yetunde sends A to Matthew and Matthew sends B to Yetunde. Ibitoye knows the values of A and B since the communication channel is insecure. The final step in this key exchange is for Yetunde and Matthew to use their secret integers to compute

$$A' \equiv B^a \pmod{p} \quad (1.3)$$

$$B' \equiv A^b \pmod{p} \quad (1.4)$$

These newly computed values A' and B' are the same and this is their exchanged key (Jeffrey, Jill & Joseph, 2008).

$$A' \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B' \pmod{p} \quad (1.5)$$

2. RELATED WORKS

A study of block ciphers algorithm was carried out by Mohan and Raji (2011). In their research, analysis of two block cipher algorithm was carried out. These algorithms include Advanced Encryption Standard (AES) and MARS algorithm. The diffusion values of AES and MARS algorithm were measured and compared. Also, the speed of these algorithms were measured. The researchers noticed that the diffusion level of MARS encryption algorithm was achieved at the end of the 5th round while that of AES was 2nd round. This means that Rijndael AES encryption algorithm is well suited to be implemented efficiently on a wide range of processors. [5] presented an analysis of ElGamal encryption system for securing data communication through the computer system.

This study was carried out in 32-bit integer computation. An experiment was performed to evaluate the maximum number of integers that can be computed in 32-bit computer system using standard 32-bit GCC compiler in Debian 6. The computing capabilities and performance measurement of the ElGamal algorithm using C language was presented by the researchers. A new alternative approach to group encodings and hash functions for ElGamal algorithm was introduced by [8]. Their proposed cryptosystem was based on new computational problems related to the Diffie-Hellman problems. This system was analyzed to have produced a better encryption ratio and remain comparable in speed with ElGamal encryption system. [9] dealt with the problem of how multiple ciphertexts can be squeezed without losing the original message information.

In their approach, the idea of decomposability for public-key homomorphic encryption was formalized. The researchers were able to prove that Elgamal encryption scheme efficiently supports decomposition. The proposed scheme was further analyzed under the standard DDH assumption. The growth in the use of Internet has called for the need to secure our information from intruders who have devised several means to unlawfully attack and modify user's information. Network intrusion detection system was developed by [12]. Gupta and Chawla [10] explored various cipher generation algorithms of cryptography that are helpful in network security. Five basic encryption algorithms were discussed in their research. These algorithms include DES, Triple DES, Blowfish, AES and RC4 which are used for block and stream ciphers.

3. METHODOLOGY

3.1 Elgamal Algorithm

In 1985, T. Elgamal introduced Elgamal asymmetric encryption algorithm (Benoit, Pascal & David, 2006). This algorithm provides an alternative to RSA algorithm for public key encryption. In public key cryptosystem, the encryption key is published and the decryption key is kept private. The various stages involved in Elgamal encryption are as follows:

Stage 1: Public key generation and Transmission

For Yetunde to communicate with Mathew, she generates her private and transmits her public keys. To do this she chooses the following parameters

- large prime number P_Y
- a primitive element α_Y
- a random integer d_Y which she keeps secret such that $2 \leq d_Y \leq P_Y$

then she generates

$$\beta_Y \equiv \alpha_Y^{d_Y} \pmod{P_Y}$$

the private key is d_Y and public key is $(P_Y, \alpha_Y,$

$\beta_Y)$

she then transmits public key to Mathew

Stage 2: Message Encryption and Transmission

For Mathew to send encrypted message to Yetunde, he does the following

- chooses random integer k which he keeps secret
- computes $r \equiv \alpha_Y^k \pmod{P_Y}$ and $t \equiv \beta_Y^k M \pmod{P_Y}$ where M is the message to be sent.
- Mathew now send encrypted message (r, t) to Yetunde

Stage 3: Message Decryption

- Yetunde needs to decrypt Mathew's ciphertext (r, t)
- Since Yetunde knows d_Y , she computes

$$z \equiv r^{d_Y} \pmod{P_Y}$$
and

$$z^{-1} \cdot t \text{ to retrieve the message } M$$

Proof

$$z^{-1} \cdot t \equiv (r^{d_Y})^{-1} \cdot t \pmod{P_Y}$$

$$\text{where } z \equiv r^{d_Y} \pmod{P_Y}$$

$$\equiv (\alpha_Y^{d_Y k})^{-1} \cdot \beta_Y^k M \pmod{P_Y}$$

$$\text{where } r \equiv \alpha_Y^k \pmod{P_Y} \text{ and } t \equiv \beta_Y^k M \pmod{P_Y}$$

$P_Y)$

$$\equiv (\alpha_Y^{d_Y k})^{-1} \cdot (M(\alpha_Y^{d_Y k})) \pmod{P_Y}$$

$$\text{where } \beta_Y \equiv \alpha_Y^{d_Y} \pmod{P_Y}$$

$$\equiv M \pmod{P_Y}$$

$$\text{where } (\alpha_Y^{d_Y k})^{-1} \text{ and } (\alpha_Y^{d_Y k}) \text{ cancelled out}$$

3.2 Flowchart of Elgamal Algorithm

The flowchart for the key generation, message encryption and message decryption using Elgamal algorithm is described as follows:

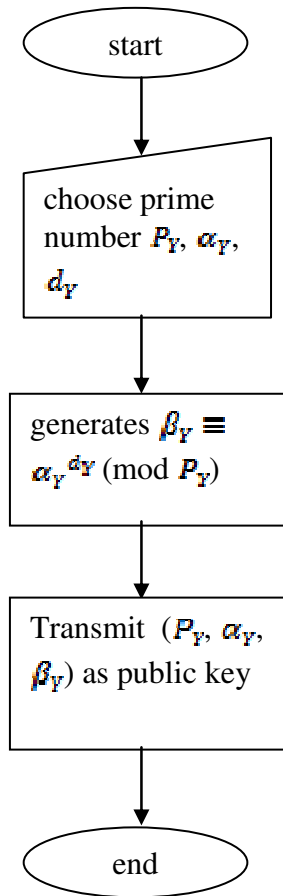


Fig 1: Public key generation flowchart

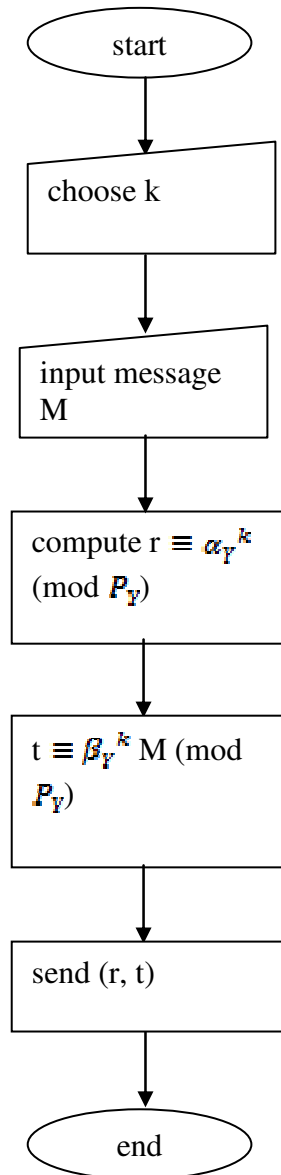


Fig 2: Message encryption flowchart

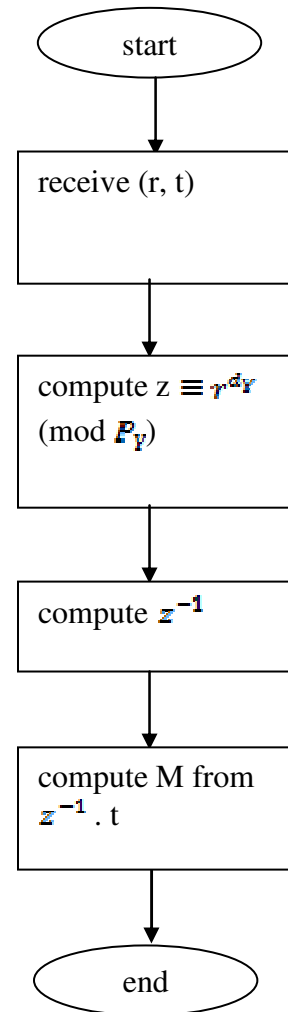


Fig 3: Message decryption flowchart

4. RESULTS AND DISCUSSION

The proposed system was implemented using Java programming language. The cryptosystem system can be used to exchange key between the sender and receiver on a network. This key can be employed in symmetric encryption or a hybrid encryption system for the purpose of sharing large files. Figure 4 shows the key generation interface. This interface is used to generate public key.



Figure 4: Public key generation interface

The encryption process is described in figure 5, 6, and 7. Elgamal algorithm uses both private key of the sender and public key of the receiver to encrypt information.



Figure 5: Elgamal algorithm requesting for sender's private key for encryption



Figure 6: Elgamal algorithm requesting for receiver's public key for encryption

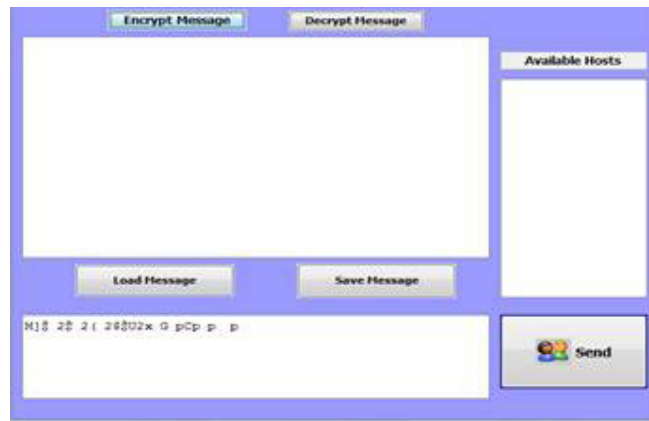


Figure 7: Encrypted information

Elgamal algorithm applies sender's public key and the receiver's private key to recover the encrypted information. The decryption process is shown in figure 8, 9 and 10.

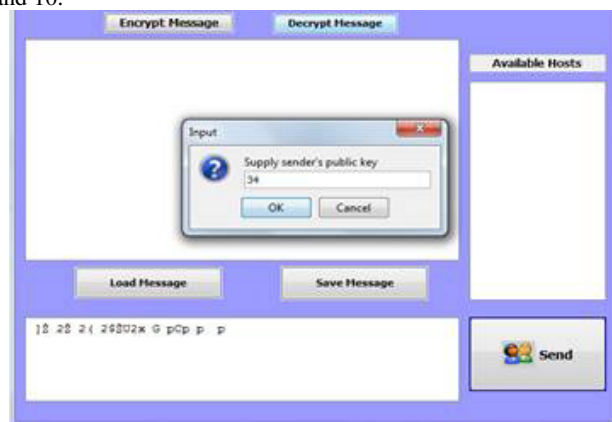


Figure 8: Elgamal algorithm requesting for sender's public key for decryption



Figure 9: Elgamal algorithm requesting for receiver's private key for decryption

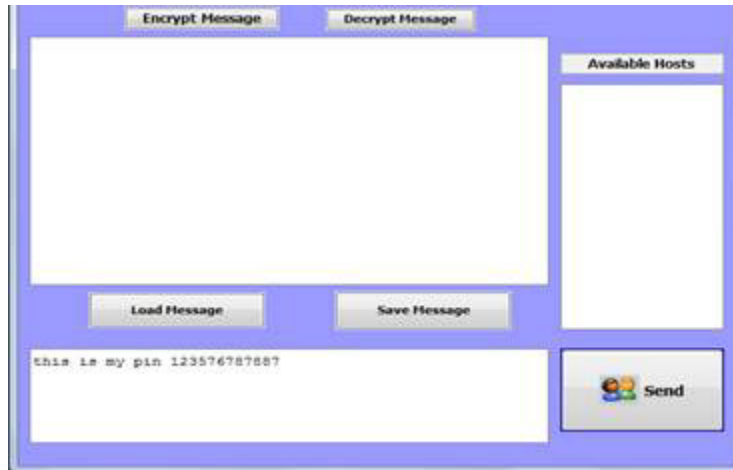


Figure 10: Decrypted information

5. CONCLUSION

Elgamal system is a public key cryptosystem that is based on discrete logarithm problem. In this paper, a network-based key exchange cryptosystem was developed using Elgamal algorithm. Elgamal algorithm used both public and private key, hence, it is asymmetric encryption algorithm. The algorithm gives a different ciphertext each time encryption is performed. However, 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 (Rajan & Geeta, 2013). The proposed system is recommended for key exchange due to the drawbacks of the algorithm for encrypting large file or messages. A further research could be done in the area of hybridization to improve the efficiency and application of the system for securing data and information.

REFERENCES

- [1] Elaine, B. B., William, C. B., and Annabelle, L. (2005): *Guideline for Implementing Cryptography in the Federal Government National Institute of Standard and Technology*, NIST Special Publication 800 – 21.
- [2] Daemen, J., and Rijmen, V. (2000). *The Block Cipher Rijndael, Smart Card Research and Applications, LNCS 1820*, Quisquater and B. Schneier, Eds., Springer-Verlag, pp. 288-296.
- [3] Bryce, A. (2008). Implementing several attacks on plain Elgamal encryption. M.Sc. Thesis in Mathematics, Iowa State University, Iowa.
- [4] Jeffrey, H., Jill, P., and Joseph H. S. (2008). *An Introduction to Mathematical Cryptography*. USA: Springer
- [5] Nurul, A. R., Mohd, Z. A., Habibah, H., Syed, F. S., Mohd, A. M. (2013). Cryptographic Computation Using Elgamal Algorithm in 32-bit Computing System, 3rd International Conference on Control, Automation and Systems Engineering, *Atlantis Press*, pp. 63-67.
- [6] ScienceDaily (2013). Cryptography, Retrieved 23rd December, 2013 from <http://www.sciencedaily.com/articles/c/cryptography.htm>
- [7] Mohan, H. S., and Raji, A. R. (2011). Performance Analysis of AES and MARS Encryption Algorithms, *International Journal of Computer Science Issues*, 8(4), pp. 363-368.
- [8] Benoit, C., Pascal, P., and David, P. (2006). *Encoding -Free Elgamal Encryption Without Random Oracles*, 9th International Conference on Theory and Practice in Public Key Cryptography. USA: Springer, pp. 91-104
- [9] Myungsun, K, Jihye, K., and Jung, H. C. (2010). Compress Multiple Ciphertexts Using Elgamal Encryption Schemes, Mathematics Subject Classification. Retrieved 20th December, 2013 from <http://www.eprint.iacr.org/2012/243.pdf>
- [10] Gupta, G., and Chawla, R. (2012). Review on Encryption Ciphers of Cryptography in Network Security. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(7), pp. 211-213
- [11] Rajan, S. J., and Geeta, S. J. (2013). File Encryption and Decryption Using Secure RSA. *International Journal of Emerging Science and Engineering (IJESE)*, 1(4), pp. 11-14
- [12] Babatunde, R. S., Adewole, K. S., Abdulsalam, S. O., and Isiaka, R. M. (2014). Development of an Intrusion Detection System in a Computer Network. *International Journal of Computers & Technology*, Council for Innovative Research, 12(5), pp. 3479-3485