Application of the ElGamal Algorithm on Information Security

[1] Heri Kurniawan, [1] Andysah Putera Utama Siahaan, [2] Prabowo
[1]Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
[2]Degree Student, Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email: [1] herikurniawan@dosen.pancabudi.ac.id, [1] andiesiahaan@gmail.com, [2] prabowoardinata@gmail.com

Abstract: *Cryptography is the art and science of hiding a message. Inside there is a process of key formation, encryption, and decryption. Encryption is the process of forming plaintext into ciphertext, while decryption is the process of converting ciphertexts into plaintext. Algorithms used in cryptography are called cryptographic algorithms and based on the types of keys used cryptographic algorithms are divided into three, namely symmetry cryptographic algorithms, cryptographic asymmetry algorithms, and hash functions. The purpose of this study is to discuss the security of text messages using one of the asymmetric algorithms, namely the ElGamal algorithm. Elgamal algorithm has a public key in the form of three pairs of numbers and a secret key in the form of a number. This algorithm performs the encryption and decryption process in plaintext blocks and ciphertext blocks are generated, each of which consists of two pairs of numbers. To create a secret message the message must be converted first in integers and then encoded based on the ASCII code. This algorithm is very well used by using large numbers.*

Keywords: *Cryptography, ElGamal, Encryption, Decryption, Ciphertext, Plaintext.*

1. INTRODUCTION:

In building computer security, a system of data or file security is needed [1]–[4]. The encoding method that was created still uses the secret algorithm method [5]. This method builds on the confidentiality of the algorithm used. However, this method is not efficient when it must be used to communicate with many people. Therefore, someone has to make a new algorithm when exchanging confidential information with other people. Because the user feels inefficient, the secret algorithm is being abandoned and introduced to a new method called the key algorithm. This method does not build security on the algorithm, but on the secrecy of the key used in the encryption process. The algorithm can be known and studied by anyone. The key algorithm method has a better level of efficiency and security compared to the secret algorithm [6]. Key algorithms known as cryptography have covered aspects of human life today [7]–[9] To maintain security that has essential confidential information, one of the information security techniques is used by using the data encryption algorithm. In this system, the ElGamal algorithm will be implemented in protecting information. According to the journal of a Public Key Cryptosystem and a Signature Based on Discrete Logarithms, the strength of the Elgamal Cryptography algorithm lies in the calculation of digital signatures that emphasize discrete algorithm calculations. Until now ElGamal cryptography is still believed to be an encoding method, such as PGP applications (Pretty Good Privacy) and GnuPG which can be used to secure e-mail and digital signatures [10]. So this final project is expected to help provide security to the data. The important information takes a long time and is difficult to solve [11]. Therefore to avoid this from happening, the author uses the ElGamal cryptographic algorithm for the process of encryption and description of data.

2. THEORIES:

2.1 Cryptography

Cryptography comes from Greek; Crypto means secret and graphical means writing. According to the terminology, cryptography is the science and art to maintain the security of messages when sent from one place to another [12]. This science and art has been used for a long time ago in the military and secret agents [13]. Moreover, until now experts continue to develop and research its use. Cryptography is the mathematical techniques related to security aspects such as validity, data integrity, and data authentication [14]. Cryptography does not only provide information security but more towards the techniques [15]. Cryptography has two essential parts, such as encryption and description. Encryption is the encoding process from the original to what cannot be interpreted as the original message. The description itself means changing the message that has been encoded into the original message [16]. Original messages are usually called plaintext, while encrypted messages are called ciphertext. The mathematical algorithm used in the encryption process is called chipper, and a system that uses cryptography to secure information systems is called a cryptosystem. There are four fundamental objectives of cryptography which are also aspects of information security, such as:

a. Secrecy is an aspect that is related to safeguarding the contents of information from anyone except those who have the authority or secret key to open information that has been encrypted.
b. Data integrity is an aspect related to guarding against unauthorized data changes. The system must have the ability to detect data manipulation by unauthorized parties to maintain data integrity, including the insertion, deletion, and subsidization of other data into the actual data.
c. Authentication is an aspect related to identification or recognition, both in a unified system and information itself. Two parties that communicate with each other must introduce themselves. The information sent must be authenticated authenticity, the contents of the data, the time of delivery, and others.
d. Non-repudiation is an attempt to prevent the denial of the transmission of information by the sender or must be able to prove that a message comes from someone if he denies sending the information.

2.2 ElGamal

The ElGamal algorithm is an asymmetric cryptographic algorithm [17]. First published by Taher ElGamal in 1985. This algorithm is based on a discrete logarithmic problem in the Zp * group. The ElGamal algorithm consists of three processes, namely the key formation process, the encryption process, and the decryption process. This algorithm is a block cipher, which is an encryption process on plaintext blocks and produces ciphertext blocks which are then decrypted, and the results are combined back into a complete and understandable message. To form the ElGamal cryptographic system, primes p, and the primitive element Zp * are needed. Elgamal algorithm has a public key in the form of three pairs of numbers, namely (p, α, β) and the secret key in the form of a number, namely (a). This algorithm has a disadvantage in ciphertexts that have twice the length of the plaintext. However, this algorithm has advantages in encryption. For the same plaintext, this algorithm gives a different ciphertext every time plaintext is encrypted.

In brief, the amount in ElGamal cryptography can be written which is used as a reference for the writing of this essay:

a. Prime numbers, p (non-confidential).
b. Random numbers, α ($\alpha < p$) (non-confidential).
c. Random numbers, a (a <p) (confidential and private key).
d. $\beta = \alpha^a \bmod p$ (is not confidential and is a public key).
e. m is plaintext (confidential).
f. γ and δ are ciphertexts (confidential).

The process as secret key cryptography. The description of the ElGamal algorithm process can be seen in the following figure [18].

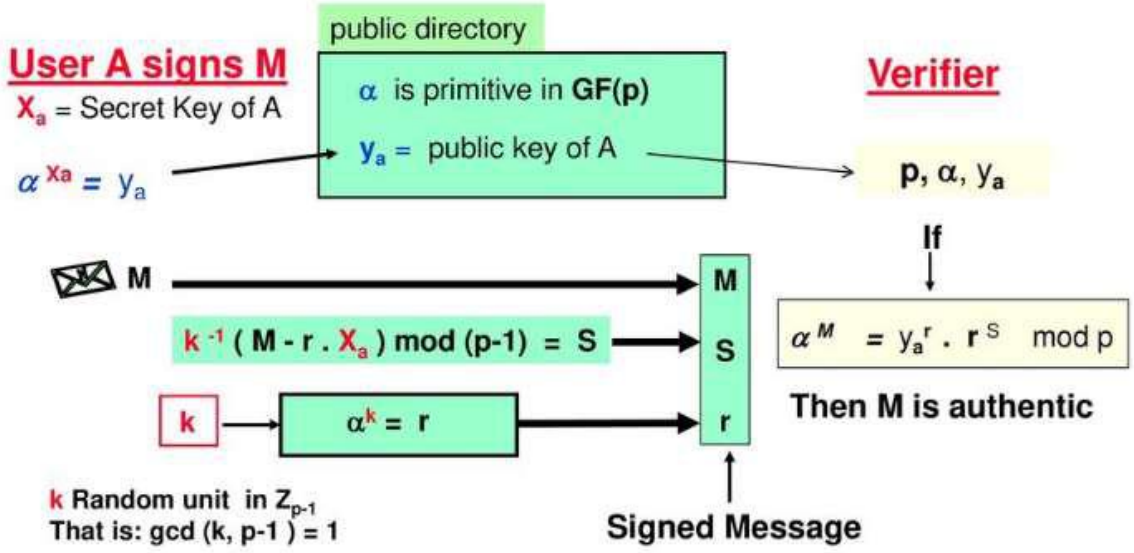

Figure 1. ElGamal Signature Scheme

3. METHODOLOGY:

3.1 Key Formation Process

Generating key pairs consisting of secret keys and public keys is the first process that must be carried out in ElGamal cryptography. The first procedure to do is to select any prime number p. Then choose two random numbers, primitive elements α and a with terms $\alpha < p$ and $a \in \{0,1,\ldots,p-2\}$. Then we can calculate $\beta = \alpha^a \bmod p$. The general

key of ElGamal cryptography is a pair of 3 numbers, such as (β, α, p) with $\beta = \alpha^a$. While the secret key to ElGamal cryptography is a pair of numbers, such as (a, p). In ElGamal cryptography using prime integers in the encryption calculation process, the message must be converted into an integer

3.2 Encryption Process

In this process, the message is encrypted using a public key (p, α, β) and any secret random number $k \in \{0.1, ..., p - 2\}$ which is kept confidential by the recipient who encrypts the message. Suppose m is a message that will be sent or ordered in plaintext form, then m characters blocks are changed, and each character is converted to integers, so the plaintext $m_i, m_2,\ldots,m_n$ with $m_i \in \{0,1,\ldots,p-2\}$, $i = 1,2,\ldots,n$. The encryption process in the ElGamal algorithm is done by these following equations.

$$\gamma = \alpha^k (\text{mod } p)$$

$$\delta = \beta^k . m (\text{mod } p)$$

3.3 Decryption Process

After receiving the ciphertext (γ, δ), the next process is to decrypt the ciphertext using public key p and secret key a. It can be shown that plaintext m can be obtained from ciphertext using a secret key a. Decryption from ciphertext to plaintext uses a secret key that is kept confidential by the recipient of the message. The decryption process can be performed by using the following equation.

$$m = \delta . (\gamma^a)^{-1} \text{ mod } p$$

4. RESULT AND DISCUSSION:

System evaluation is performed to show whether the system that has been designed can run as expected. Also, the purpose of the test is to be able to find a function error in the application that was built and fix it. Tests are carried out by entering characters or letters from text format files then processed by the application whether the application can provide the appropriate results. The process to be tested in this application is the recipient can read a message delivery simulation using the ElGamal algorithm method between the sender to the recipient with the key that is owned by each party without the need to exchange a single key until the original message sent by the sender. The following tables describe the encryption process from the plaintext.

Table 1. Plaintext

No.	Char	Plaintext m(i)	ASCII
1	k	m1	107
2	a	m2	97
3	m	m3	109
4	p	m4	112
5	u	m5	117
6	S	m6	115

Table 2. Encryption Result

I	mi	ki	$\gamma = 2^{ki} \, mod \, 2579$	$\delta = 949^{ki} . mi \, mod \, 2579$
1	107	766	1898	342
2	97	2298	520	1516
3	109	146	22	359
4	112	2483	1742	830
5	117	702	1052	1302
6	115	988	2153	2087

The Sender sends the results of the ciphertext to the recipient. When received, the recipient must decrypt the ciphertext so that the recipient has the public key p = 2579 and secret key a = 765 to decrypt the ciphertext according to the decryption algorithm.

Table 3. Decryption Result

No.	$(\gamma i, \delta i)$	$\gamma i^{1813} \bmod 2579$	$mi = \delta i . \gamma i^{1813} \bmod 2579$	Char
1	(1898, 342)	219	107	k
2	(520, 1516)	1771	97	a
3	(22, 359)	1825	109	m
4	(1742, 830)	286	112	p
5	(1052, 1302)	422	117	u
6	(2153, 2087)	655	115	s

5. CONCLUSION:

Based on the discussion in the design of the application of the ElGamal Algorithm in securing information, it can be concluded. The use of the ElGamal Algorithm is well used for data security processes. The possibility of key leakage when the process of exchanging single key information can be complicated to know. This algorithm has good mathematical calculations. The disadvantage of this algorithm is that the resulting ciphertext will have higher capacity than the initial plaintext. The higher the value in the public and private key, the higher the value of the ciphertext that is generated. It is difficult to convert numbers to characters to store the ciphertext.

REFERENCES:

1. Andre Hasudungan Lubis, S. Z. S. Idrus, and A. Sarji, "ICT Usage Amongst Lecturers and Its Impact Towards Learning Process Quality," *Malaysian J. Commun.*, vol. 34, no. 1, pp. 284–299, 2018.
2. M. I. Perangin-Angin, A. H. Lubis, I. S. Dumayanti, R. B. Ginting, and A. P. U. Siahaan, "Implementation of Fuzzy Tsukamoto Algorithm in Determining Work Feasibility," *IOSR J. Comput. Eng.*, vol. 19, no. 4, pp. 52–55, 2017.
3. M. D. L. Siahaan, Elviwani, A. B. Surbakti, A. H. Lubis, and A. P. U. Siahaan, "Implementation of Simple Additive Weighting Algorithm in Particular Instance," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, pp. 442–447, 2017.
4. S. Haryati, A. Ikhwan, D. Arisandi, Fadlina, and A. P. U. Siahaan, "Quality Assurance in Knowledge Data Warehouse," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, p. 239–242], 2017.
5. H. Ming and S. LiZhong, "A New System Design of Network Invasion Forensics," in *2009 Second International Conference on Computer and Electrical Engineering*, 2009, pp. 596–599.
6. A. P. U. Siahaan, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," *Int. J. Adv. Appl. Sci.*, vol. 6, no. 4, pp. 313–318, 2017.
7. A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *Int. J. Sci. Res.*, vol. 5, no. 7, pp. 1149–1152, 2016.
8. M. D. L. Siahaan and A. P. U. Siahaan, "Application of Hill Cipher Algorithm in Securing Text Messages," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 55–59, 2018.
9. M. Iqbal, A. P. U. Siahaan, and R. P. Sundari, "Combination of MD5 and ElGamal in Verifying File Authenticity and Improving Data Security," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 96–101, 2018.
10. F. H. Khan, R. Shams, F. Qazi, and D.-E.-S. Agha, "Hill Cipher Key Generation Algorithm by using Orthogonal Matrix," *Int. J. Innov. Sci. Mod. Eng.*, vol. 3, no. 3, pp. 5–7, 2015.
11. A. Lubis and A. P. U. Siahaan, "Network Forensic Application in General Cases," *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 41–44, 2016.
12. W. Stallings, *Cryptography and Network Security Principles and Practices*, 4th ed. Prentice Hall, 2005.
13. A. Putera Utama Siahaan, E. Elviwani, and B. Oktaviana, "Comparative Analysis of RSA and ElGamal Cryptographic Public-key Algorithms," in *Proceedings of the Joint Workshop KO2PI and The 1st International Conference on Advance & Scientific Innovation*, 2018.
14. A. P. U. Siahaan, "A Fingerprint Pattern Approach to Hill Cipher Implementation."
15. A. P. U. Siahaan, *How to Code: Advanced Encryption Standard in C#*. Medan: Fakultas Ekonomi Universitas Panca Budi, 2018.
16. Y. Kumar, R. Munjal, and H. Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures," *Int. J. Comput. Sci. Manag. Stud.*, vol. 11, no. 3, pp. 60–63, 2011.
17. B. Forouzan, *Cryptography and Network Security*. New York, NY, USA: McGraw-Hill, 2006.
18. Corey Houston, "Public-Key Cryptography ElGamal Public-Key Crypto-System," *Slide Player*, 2018. [Online]. Available: https://slideplayer.com/slide/12448138/. [Accessed: 13-Nov-2018].