Modification of chipertext Elgamal algorithm using split merge

Rahmadi Asri, Mahyuddin K.M Nasution, Suherman Suherman

Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Medan, Indonesia
*Email: rahmadi2808@gmail.com

Abstract—The development of increasingly sophisticated technology with more intensive use of computers facilitates human work activities, so that security problems arise that misuse information that can endanger users. The third parties who commit crimes against users are called cryptanalyst. Cryptanalyst interferes with computer networks in many forms such as data theft. Cryptography is a security solution for cryptanalysts; one of them is by using the El-Gamal algorithm. Researchers have proposed El-Gamal modification with good results, but not all security problems can be solved. The algorithm cannot guarantee protection against the adaptive attack. This article proposes the application of split merge method on the El-Gamal algorithm to improve security. The study describes the system analysis and design. Since the combination uses large prime number calculations, it is expected to be effective to make cryptanalyst more difficult to break the plaintext.

1. Introduction

The development of science and technology is increasingly sophisticated with increasingly intensive use of computers to assist human work, both in the government and private sectors. However, security problems arise as the information processed by the computer can be misused, both computer security independently and network security [1]. Security problems can be in the form of tampering, phishing, trojans, denial of services attacks, man in the middle attacks and others [12,13,14,15].

One of the security solutions is cryptography. Cryptography is the science of converting original messages into secret messages. The message has been given a password by the sender of the message, so that the message can be read by the recipient using a certain key [11]. There are several data security algorithms so that the data cannot be read by cryptanalysts. The encoded data is known as chipertext.

There are two types of keys, consisting of symmetrical keys and asymmetric keys [2]. These two types of cryptographic keys have advantages and disadvantages when processing data encryption and description of data.

El-Gamal is one of the popular cryptographic algorithms. In general, the El-Gamal algorithm is used to encrypt messages. The El-Gamal algorithm includes a simple and efficient cryptographic algorithm [3]. This algorithm can do a large number of factoring, so it is quite safe to calculate key formation by using random numbers. For this reason, El-Gamal is able to maintain message security from cryptanalyst attacks.

Research that developed the El-Gamal algorithm has been carried out. The El-Gamal modification by [4] proofs that the merging of sequential methods and parallel schemes on encryption improve
security and systematically secures messages from cryptanalyst attacks. Research by [5], which compared the MECA cryptosystem with El-Gamal, stated that the El-Gamal Algorithm could not be used for authentication as El-Gamal was not safe against adaptive attacks. As a solution, this article offers a solution using the split merge method which aims to separate and recombine the plaintext. Split merge research is done by [6] where split merge is applied to an image that is split (split) and then merged again, to find an object. In this study the author uses the split merge method in the encryption method of a plaintext in cryptography so that cryptanalysts have difficulty reading the plaintext.

2. Research background

Security research has been carried out in cryptographic studies, one of which is the El-Gamal algorithm, the application of the El-Gamal algorithm to cryptographic systems to prevent attacks on cryptanalysts, attacks on networks such as websites and online sites and attacks on text, image, sound and video file data. Some researchers have conducted research on cryptographic studies in the El-Gamal Algorithm as follows.

| NO | EL-GAMAL RESEARCH | TOPIC | AUTHOR | RESULT |
|----|--------------------|-------|--------|--------|
| 1. | A Cryptographic Approach Based On Integrating Running key in Feedback Mode Of ElGamal System [2] | Priya Nalwaya Varun P Saxena Pulkit Nalwaya (2014) | High security enhancements can affect the process speed of the processor |
| 2. | ElGamal Algorithm for Encryption of Data Transmission [3] | Zengqiang Wu Di Su Gang Ding (2014) | the application of the public key to the transmission can maintain good information |
| 3. | Modified El Gamal Algorithm for Multiple Senders and Single Receiver Encryption [4] | Aris J. Ordonez and Ruji P. Medina, Bobby D. Gerardo | Merging sequential methods and parallel schemes on encryption is very good and can systematically secure messages from cryptanalysis attacks |
| 4. | Modified Elgamal Cryptosystem Algorithm (MECA) [5] | Prashant Sharma, Sonal Sharma, Ravi Shankar Dhakar (2011) | El-Gamal algorithm is not safe against adaptive attacks |
| 5. | Split And Merge Approach For Detecting Multiple Planes In A Depth Image [6] | Seon-Min Rhee, Yong-Beom Lee, James D. K. Kim, Taehyun Rhee (2012) | Split and Merge implementations can detect an object in the image |
| 6. | Implementation of ElGamal Elliptic Curve Cryptography Over Prime Field Using C [7] | Debabrat Boruah, Monjul Saikia 2014 | El-Gamal implementation - Elliptic Curve Cryptosystem uses c language, in very good security settings |
| 7. | Design and Implementation Stegocrypto Based on ElGamal Elliptic Curve [8] | Litasari, Budi Rahadjo 2017 | Stegocrypto implementation managed to increase security against cryptanalyst attacks |

3. Methodology

3.1 Method of Split - Merge

Split merge method is a grouping process of bits in plaintext which is separated into four parts consisting of q1, q2, q3, q4 and the key in the plaintext is divided into two parts consisting of s1, s2. The separation of bits can be seen in the table below [10]:

| Method Split | Method Merge |
|--------------|--------------|
| Plaintext    | q1 | q2 | q3 | q4 | s1 | s2 | q3 | q4 | s1 | s2 | q3 | q4 | s1 | s2 | Cipher text |
| q1 | q2 | q3 | q4 | s1 | s2 | q3 | q4 | s1 | s2 | q3 | q4 | s1 | s2 | |
| 01 | 01 | 00 | 10 | 01001100 | 01000100100010100 | 11000011001100101100 | 1000011001100101100 |
| Key | s1 | s2 | 0100 | 1100 | 01000100100010100 | 11000011001100101100 | 1000011001100101100 |

2
As shown in Table 2, split merge produces ciphertext four times larger than plaintext when one character letter (plaintext) produces four character letters (ciphertext).

3.2 El-Gamal algorithm

El-Gamal algorithm was created in 1976, used for data security. Its security lies in the calculation of algorithms using large primes. There are three levels of process which consist of key formation, encryption and description processes [9].

1. The formation of the Key of the El-Gamal Algorithm consists of the public key \((p, g, y)\) and private key \((x, p)\) Determine the key generation:
   1.1 select prime random number \((p)\)
   \(p = 103\)
   1.2 Determine the value \(g\), \(g < p\)
   \(g = 5\)
   1.3 Select random numbers \(2 \leq x \leq p - 1\)
   \(X = 11\)
   1.4 \(g\) and \(x\) smaller than \(p\), calculate the value of \(y = g^{x} \mod p\)

2. Encryption process, conditions of the encryption process as follows
   2.1 Arrange the original message into blocks - blocks \(m_1, m_2, \ldots, m_n\)
   2.2 Change the value of the original message into ASCII
   2.3 Select random numbers \(k\), with the condition \(1 \leq k \leq p - 2\)
   2.4 Calculate the value of \(a = g^{k} \mod p\) and \(b = y^{m} \mod p\)
   2.5 Arrange ciphertext with formulas \(a_1, b_1, a_2, a_2, \ldots, a_n, b_n\)

3. Description process
   3.1 takes the value of ciphertext which has been encrypted
   3.2 calculates the value of ciphertext using the formula \(C_n = b_i \cdot a_i \cdot (p - 1 - x) \mod p\)
   3.3 arranges the plaintext value sequentially \(m_1, m_2, \ldots, m_n\)

The flow of encryption is the process of encoding the plaintext, the plaintext that has been encoded by the El-Gamal algorithm is called ciphertext, the ciphertext is secured by the split method by separating the ciphertext in the form of bits then put together back to its original shape.

![Figure 1. Encryption and Description](image-url)
4. System Analysis and Design

El-Gamal algorithm is one of the popular algorithms where the security of this algorithm lies in the difficulty of calculating large logarithms, this El-Gamal algorithm can also increase the security of messages against cryptanalyst attacks whose purpose is to damage computer systems and computer networks as a whole, threats to computer networks such as websites and online sites [16,17].

The application of split merge on the El-Gamal algorithm is as follows:

4.1 Key generation

Selection of keys uses random:
- Key primes (\(y = 48, g = 5, p = 103\))
- Private Key (\(x = 11, p = 103\))

\[
y = g^x \mod p = 5^{11} \mod 103 = 48
\]

4.2 Encryption

Alphabet A used for encryption with the steps as follows:

| Table 3. Character Conversion into ASCII |
|-----------------|-----------------|
| No | Character | Plaintext (ASCII) |
|---|----------|-------------------|
| 1 | A | 65 |

Specify random numbers according to the provisions of \(1 \leq k \leq p-2\)

| Table 4. Value of k (random number) |
|-----------------|-----------------|
| No | mi | K |
|---|---|---|
| 1 | 65 | 29 |

Then, encrypt plaintext by using the formula \(a = g^k \mod p\), to calculate the value of \(a\)

\[
a = g^k \mod p = 5^{29} \mod 103 = 84
\]

After that use the formula \(b = y^k \cdot m \mod p\), to calculate the value of \(b\)

\[
b = y^k \cdot m \mod p = 48^{29} \cdot 65 \mod 103 = 29
\]

So the encryption value in character (A) produces chipertext \(a = 84\) and \(b = 29\). Further, the results of a and b encryption are separated, for chipertext a to be four parts and chipertext b becomes four parts.
Table 5. Split

| Character | ASCII | Binary | Group Distribution |
|-----------|-------|--------|--------------------|
| Plaintext (a) | T | 84 | 01010100 | q1 | q2 | q3 | q4 |
| Key | 0 | 48 | 00110000 | s1 | s2 |
| Plaintext (b) | GS | 29 | 00011101 | 00 | 01 | 11 | 01 |
| Key | 0 | 48 | 00110000 | 0011 | 0000 |

After a split with a separate key reunited in the provisions as follows:

Table 6. Merge

| Merger Rules | Implementation | Results | Merger Rules | Implementation | Result |
|--------------|----------------|---------|--------------|----------------|--------|
| Plaintext (a) | N. = q1 s1 q1 ; N. = 01 0011 01 01001101 | N. = q1 s1 q1 ; N. = 00 0011 00 01001100 |
| N. = q2 s2 q2 ; N. = 01 0011 01 01001101 | N. = q2 s2 q2 ; N. = 01 0011 01 01001101 |
| N. = q3 s2 q3 ; N. = 01 0000 01 01000001 | N. = q3 s2 q3 ; N. = 11 0000 11 11000011 |
| N. = q4 s2 q4 ; N. = 00 0000 00 00000000 | N. = q4 s2 q4 ; N. = 01 0000 01 01000001 |
| N. = q4 s2 q4 ; N. = 00 0000 00 00000000 | N. = q4 s2 q4 ; N. = 01 0000 01 01000001 |

Then the values of N1, N2, N3, N4 are XOR with the Key Y = 48

Table 7. XOR Encryption Process

| Split - Merge | N1 | N2 | N3 | N4 | Split - Merge | N1 | N2 | N3 | N4 |
|---------------|----|----|----|----|---------------|----|----|----|----|
| Key | 00110000 | 00110000 | 00110000 | 00110000 | Key | 00110000 | 00110000 | 00110000 | 00110000 |
| XOR | 01111101 | 01111101 | 01110001 | 01110001 | XOR | 01111100 | 01111101 | 01110001 | 01110001 |
| Chipertext (a) | q | q | q | q | Chipertext (b) | q | q | q | q |

4.3 Decryption

Decryption of the opposite of encryption where the original message (plaintext) that has been encoded (chipertext) is returned to its original form so that the message can be read by XOR against the chipertext and key, as in the table below:

Table 8. XOR Decryption Process

| Chipertext (a) | N1 | N2 | N3 | N4 | Chipertext (b) | N1 | N2 | N3 | N4 |
|---------------|----|----|----|----|---------------|----|----|----|----|
| ASCII Binary Number | 01111101 | 01111101 | 01110001 | 01110001 | ASCII Binary Number | 01111100 | 01111101 | 01110001 | 01110001 |
| Key | 00110000 | 00110000 | 00110000 | 00110000 | Key | 00110000 | 00110000 | 00110000 | 00110000 |
| XOR | 01001101 | 01001101 | 01000001 | 01000001 | XOR | 00001100 | 00001100 | 00001100 | 00001100 |
| Plaintext (a) | 1 | 1 | 0 | 0 | Plaintext (b) | 1 | 1 | 0 | 0 |

The results of the Plaintext are cut by taking 2 digits N1, N2, N3, N4 from the left and 2 digits N1, N2, N3, N4 from the right, just like the picture below
The process of merging values from q1, q2, q3, q4 together, so that the plaintext that has been repacked is found again.

5. Conclusion and future work

After analyzing the El-Gamal algorithm using the split-merge method, it can be concluded that the plaintext encrypted by El-Gamal produces ciphertext 200% larger than plaintext. The ciphertext in ElGamal is separated into four ciphertext parts a and four ciphertext b, so that the text increases to eight times. If the message is encoded by layered security, it will be very difficult to be solved by the cryptanalyst.

References

[1] C Nan. 2010. Automated Security Proof of the ElGamal Encryption Scheme. In Proc. Int. Conf. on Future Computer and Communication.

[2] P Nalwaya, VP Saxена. 2014. A Cryptographic Approach Based On Integrating Running key in Feedback Mode Of ElGamal System. In Proc. Sixth Int. Conf. on Computational Intelligence and Communication Networks.

[3] Z Wu, D Su, G Ding. 2014. ElGamal Algorithm for Encryption of Data Transmission. In Proc. of Int. Conf. on Mechatronics and Control (ICMC)

[4] AJ Ordonez, RP Medina, BD Gerardo. 2018. Modified El Gamal Algorithm for Multiple Senders and Single Receiver Encryption. Vol. 978-1-5386-3527-8.

[5] P Sharma, S Sharma, RS Dhakar. 2011. Modified Elgamal Cryptosystem Algorithm (MECA). In Proc. of Int. Conf. on Computer & Communication Technology.

[6] SM Rhee. 2012. Split And Merge Approach For Detecting Multiple Planes In A Depth Image. ICIP.

[7] D Boruah, M Saikia. 2014. Implementation of ElGamal Elliptic Curve Cryptography Over Prime Field Using C. ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India.
[8] RB Litasari. 2017. Design and Implementation Stegocrypto Based on ElGamal Elliptic Curve. International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITSEE).

[9] NMS Iswari. 2018. Key Generation Algorithm Design Combination of RSA and ElGamal Algorithm. International Conference on Information Technology and Electrical Engineering (ICITEE)

[10] P Utomo. 2017. Algoritma Split-Merge One Time Pad Dalam Peningkatan Enkripsi Data. Seminar Nasional Teknologi Informatika.

[11] F Fujun, L Xinshe, W Litao. 2016. Design and Implementation of Identity Authentication System Based on Fingerprint Recognition and Cryptography. International Conference on Computer and Communications.

[12] CM Wu. 2013. Multi-Level Tamper Detection And Recovery With Tamper Type Identification. ICIP.

[13] G Doychev and B Kopf. 2015. Rational Protection Against Timing Attacks. Computer Security Foundations Symposium.

[14] C Wei. 2013. MAC Token Based on WSS Defending Web Service DoS Attacks. International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC).

[15] J Fran. 2014. A Security Engineering Process for Systems of Systems using Security Patterns.

[16] H Tao, J Zhou, S Liu. 2017. A survey of network security situation awareness in power monitoring system.

[17] JH Lee. 2017. Toward the SIEM Architecture for Cloud-based Security Services. Conference on Communications and Network Security (CNS): IEEE CNS 2017 – Posters.