PAPER • **OPEN ACCESS**

Hybrid Cryptosystem Combination Algorithm Of Hill Cipher 3x3 and Elgamal To Secure Instant Messaging For Android

To cite this article: Dian Rachmawati *et al* 2019 *J. Phys.: Conf. Ser.* **1235** 012074

IOP Conf. Series: Journal of Physics: Conf. Series **1235** (2019) 012074 doi:10.1088/1742-6596/1235/1/012074

Hybrid Cryptosystem Combination Algorithm Of Hill Cipher 3x3 and Elgamal To Secure Instant Messaging For Android

Dian Rachmawati[1*], Amer Sharif[1*], and Ericko[1*]

[1]Departemen Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Jl. Universitas No. 9-A, Medan 20155, Indonesia

[*]Email: dian.rachmawati@usu.ac.id, amersharifdjamin@gmail.com, erickooo96@gmail.com

Abstract. Instant messaging is commonly used in communication, which made a high level of security as an essential part. To secure the huge amount of messages, one of the techniques used is hybrid cryptosystem. A Symmetric Hill Cipher 3x3 and ElGamal Asymmetric Algorithm combination will be used to perform the hybrid encryption scheme. Symmetric Hill Cipher with a square 3x3 key matrix for the encryption process and ElGamal Asymmetric for encrypt the key of Hill Cipher. The strength of Asymmetric ElGamal is the difficulty of calculating discrete logs in a large prime modulus. In this research, the running time is directly proportional to the length of text during the encryption and decryption process.

1. Introduction

Cryptography is a mathematical science with data encoding techniques to secure information. The word cryptology is made up of the two components “hidden” and “study” and refers to the study of hidden writings or secrets [3]. Original message can be revealed only after decrypting the encrypted message. Generally, the cryptographic systems can be classified into symmetric and asymmetric [4].

Hybrid cryptosystem scheme is used to improve the security of data. In the hybrid cryptosystem, a file is secured by using the symmetric algorithm and symmetric key is secured by using the asymmetric algorithm [8].

Hill Cipher is a symmetric algorithm. It was developed by the mathematician Hill in 1929. In symmetric algorithms, it only uses one key to perform encryption and decryption process. The key must be known in advance to both sender and receiver before the message is being transmitted between the sender and receiver [5]. The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible matrices of size n×n (modulo 26).

ElGamal encryption is one of many encryption schemes which utilizes randomization in the encryption process [7]. The public key of ElGamal is used for encryption, and the private key is used for the decryption process. ElGamal is based on the difficulty of calculating discrete logs in a large prime modulus [1]. The security of ElGamal cryptosystem maybe compromised broken by two attacks based on low modulus and known-plaintext attacks [6].

2. Method

In this implementation the public and private key will be generated, encryption and decryption data will be sent to google firebase. Process steps are as below.

2.1 Steps for generating ElGamal key:

1. Randomize a large prime number p.

2. Get integer α as the primitive group
3. Randomize an integer d such that 1 <d<p-2 .
4. Compute $\beta = \alpha^d$ mod p.
5. Get the public key (p,α, β) and private key (d).

2.2 Steps for encryption messages:
1. Get all the plaintext and convert into ASCII.
2. Get the key of Hill Cipher 3x3.
3. Calculate the process C = K.P mod 256

2.3 Steps for encrypting the key:
1. Get the public key (p,α, β).
2. Convert the key into value (P) on each block.
3. Calculate $c_1 = \alpha^r mod\ p$ and $c_2 = P\ x\ \beta^r mod\ p$
4. Repeat the process until the key matrix of [2,2]

2.4 Steps for decrypting the key:
1. Get the private key (d).
2. Decryption on each block using $P = c_2 \times {c_1}^{p-1-d}$ mod p.
3. Repeat the process until the key matrix of [2,2]

2.5 Steps for decrypting messages:
1. Get the Inverse of Hill Cipher.
2. Calculate the process $P = K^{-1}.C$ mod 256

The encryption text from Hill Cipher :

1. Encryption Process Hill Cipher
   a. Get the plaintext and convert into the ASCII: $P = \begin{bmatrix} 4 & 1 & 7 \\ 8 & 0 & 5 \\ 10 & 3 & 2 \end{bmatrix}$
   b. Get the key Hill Cipher key 3x3: $K = \begin{bmatrix} 1 & 2 & 11 \\ 5 & 4 & 10 \\ 7 & 3 & 9 \end{bmatrix}$
   c. Calculate the process C = K.P mod 256

   Get the result : C = $\begin{bmatrix} 1 & 2 & 11 \\ 5 & 4 & 10 \\ 7 & 3 & 9 \end{bmatrix} x \begin{bmatrix} 4 & 1 & 7 \\ 8 & 0 & 5 \\ 10 & 3 & 2 \end{bmatrix}$

   $$\mathrm{C} = \begin{bmatrix} 130 & 34 & 39 \\ 152 & 35 & 75 \\ 142 & 34 & 82 \end{bmatrix}$$

2. Generate Key
   a. Randomize a prime number p = 241
   b. Get α = 7
   c. Randomize d = 13.

   β = α^d mod p
   = 7^{13} mod 256
   = 199

   d. Then get the public key (p,α,β) = (241,7,199) and private key (d) = (13).

3. Key Encryption Process
   a. Get the public key (p,α,β) = (241,7,199).
   b. Randomize $r < p - 1$. r = 30.
   c. Calculate c_1 and c_2 on each block

   C_1 [0,0] = α^r mod p
   = 7^{30} mod 241
   = 30

   C_2 [0,0] = P_1 x β^r mod p
   = 1 x 199^{30} mod 241

= 211

C_1 [0,1] = $\alpha^r \bmod p$
= $7^{30} \bmod 241$
= 30

C_2 [0,1] = $P_1 \times \beta^r \bmod p$
= $2 \times 199^5 \bmod 241$
= 181

d. Repeat the process until the key matrix of [2,2]

e. The result of a key encryption process showed in table 1.

Table 1. Encryption Key

Key	C_1	C_2
[0,0]	30	211
[0,1]	30	181
[0,2]	30	152
[1,0]	30	91
[1,1]	30	121
[1,2]	30	182
[2,0]	30	31
[2,1]	30	151
[2,2]	30	212

4. Key Decryption Process
   a. Get the private key (d) = (13).
   b. Decryption on each block with calculate $P = c_2 \times c_1^{p-1-d} \bmod p$.

$P_1[0,0]$ = $c_2[0,0] \times c_1\ [0,0]^{\,p-1-d} \bmod p$
= $211 \times 30^{241-1-13} \bmod 241$
= 1

$P_2[0,1]$ = $c_2[0,1] \times c_1\ [0,1]^{\,p-1-d} \bmod p$
= $181 \times 30^{241-1-13} \bmod 241$
= 2

   c. Repeat the process until the key matrix of [2,2]

d. The result of the key decryption process showed in table 2.

Table 2. Decryption Key

Key	P
[0,0]	1
[0,1]	2
[0,2]	11
[1,0]	5
[1,1]	4

[1,2]	10
[2,0]	7
[2,1]	3
[2,2]	9

5. Decryption Process Hill Cipher
   a. Get the inverse key of Hill Cipher: $K^{-1} = \begin{bmatrix} 150 & -9 & 168 \\ -15 & 92 & -27 \\ 59 & -109 & 106 \end{bmatrix}$
   b. Calculate the process P = $K^{-1}\ x\ C\ mod\ 256$

$$= \begin{bmatrix} 150 & -9 & 168 \\ -15 & 92 & -27 \\ 59 & -109 & 106 \end{bmatrix} x \begin{bmatrix} 130 & 34 & 39 \\ 152 & 35 & 75 \\ 142 & 34 & 82 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 4 & 1 & 7 \\ 8 & 0 & 5 \\ 10 & 3 & 2 \end{bmatrix}$$

6. Firebase
   All of the public key and private key that has been generated by ElGamal will be send to google firebase. The generated key and result of the data encryption showed in figure 1 and figure 2 as below.

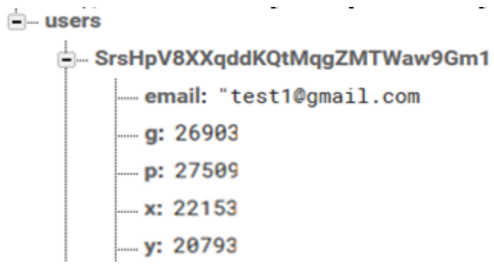

Figure 1. The public key and private key

Figure 2. Encryption data on firebase

3. Results and Discussions

The experiments were performed on smartphone Android version 6.0 RAM 4gb Processor 1.5GHz Octa-core. The screenshot of the application showed in figure 3 as below.

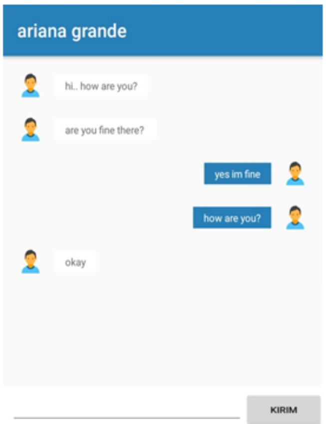

Figure 3. Chatting Room

The results of the running time encryption and decryption for every different length of text showed in table 3 and table 4 as below.

Table 3. The running time for the encryption process of 5 different lengths of text.

Length / Session	**Processing time (*millisecond*)**					
	1	**2**	**3**	**4**	**5**	**Average**
100	86.795385	67.679231	82.464154	75.930154	67.307154	76.0321
200	88.773615	75.389616	75.029154	100.915616	77.875	83.59659
500	102.093461	102.381616	68.709923	73.007154	89.236461	87.08542
1000	131.514154	94.25623	86.161847	79.985	68.395307	92.0623
2000	86.514077	113.894615	94.961384	119.813077	101.587769	103.353

The graphic of running time process encryption showed in figure 4 as below.

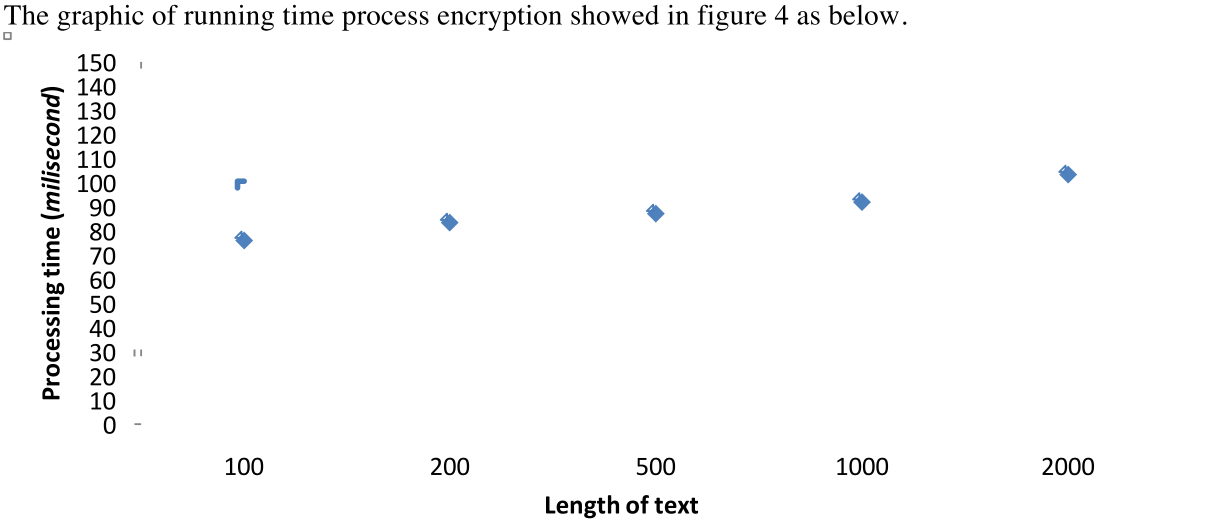

Figure 4. Graphic time of encryption

Table 4 The running time for the decryption process of 5 different lengths of text.

Length / Session	Processing time (*millisecond*)					
	1	2	3	4	5	Average
100	4.129615	4.566308	4.450847	4.145385	4.212308	4.3008926
200	5.391	5.201	5.60281	5.125769	5.271692	5.318454
500	17.259615	17.199077	18.326823	20.783154	20.830692	18.879872
1000	26.851385	27.193615	25.979923	26.737615	29.789538	27.3104152
2000	47.824	47.353769	48.212385	46.969308	48.1689	47.705672

The graphic of running time process encryption can be seen in figure 5 as below.

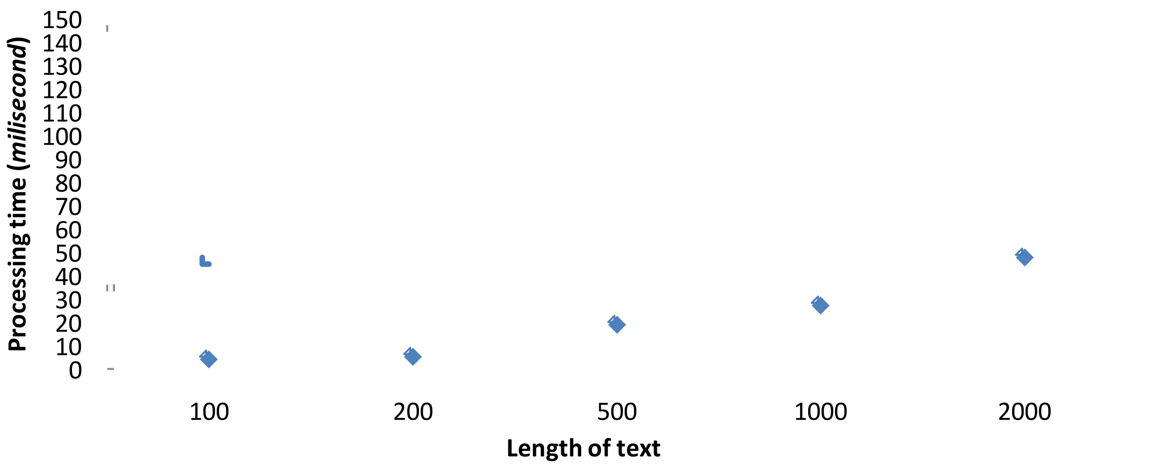

Figure 5. Graphic time of encryption

4. Conclusions

In conclusion, the time of encryption and decryption is proportional to the length of words. The average running time encryption process is 90ms and decryption process 20ms.

5. Acknowledgments

The authors gratefully acknowledge that the present research is supported by Fund Dissemination IPTEKS Research Results for Lecturers / Researchers Universitas Sumatera Utara.

References

[1] Dian Rachmawati et al 2018 IOP Conf. Ser.: Mater. Sci. Eng. 300 012040

[2] Borozdieva, Adriana 2016 MS Excel-Based Application for Encryption and Decryption of English Texts with the Hill Cipher on the Basis of 3×3-Matrix Proc. XXV International Scientific Conference Electronics - ET2016, September 12 - 14, 2016 Sozopol Bulgaria

[3] Batten, Lynn Margaret 2013 Public Key Cryptography Application and Attacks New Jersey : John Wiley & Sons, Inc

[4] Maholtra, Mini.2014 A New Encryption Scheme Based on Enhanced RSA and ElGamal International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS). ISSN (Print): 2279-0047 ISSN (Online): 2279-0055

IOP Conf. Series: Journal of Physics: Conf. Series **1235** (2019) 012074 doi:10.1088/1742-6596/1235/1/012074

[5] Mani, Mahendran 2017 Generation of Key Matrix for Hill Cipher Encryption Using Classical Cipher

[6] Sharma, Prashant, et all 2012 Intensified ElGamal Cryptosystem (IEC) International Journal of Advances in Engineering & Technology Jan 2012 SSN: 2231-1963

[7] Singh, Rashmi, Shiv Kumar 2012 Elgamal's Algorithm in Cryptography International Journal of Scientific & Engineering Research Volume 3, Issue 12, December-2012. ISSN 2229-5518.

[8] Dian Rachmawati et al 2018 IOP Conf. Ser.: Mater. Sci. Eng. 300 012042