Design of Web Login Security System using ElGamal Cryptography

Yudhi Arta, Hendra Pratama, Apri Siswanto, Abdul Syukur and Panji Rachmat Setiawan
Department of Informatics Engineering, Universitas Islam Riau, Pekanbaru, Indonesia

Keywords: Web Login, ElGamal, Cryptography.

Abstract: The login system is a process for accessing a computer by entering the identity of the user and the password to obtain permissions using the destination computer resources. In an information system security issues and maintaining data confidentiality is one important aspect. However, these security issues often get less attention from the owners and managers of information systems. If talking about security issues related to the use of computers, it is difficult to separate it with the login process. Login aims to provide security services on the system. In this research used ElGamal cryptography algorithm to secure username and password in web login. The security level of this algorithm is based on the problem of discrete logarithms in the multiplication group of prime modulo primes. This algorithm includes asymmetric cryptography algorithms that use two key types, namely public key and secret key. The data contained in the login is secured by using ElGamal algorithm, so the username and password entered into the database are already in the form of ciphertext.

1 INTRODUCTION

The login system is the process of accessing a computer by entering the identity of the user and password to get access rights using the destination computer resources. When logging in to enter the system, the user will be asked to enter a user identity such as user id and password in anticipation of system security. Passwords can be changed according to needs while user id is never changed because it is a unique identity that refers to a particular user.

Information system on security issues and maintaining data confidentiality is one important aspect. But this security problem often gets less attention from the owners and managers of information systems (Arta et al., 2018). Security issues are second or even last in the list of things that are considered important(Arta, 2017; Novendra et al., 2018).

Internet users, usually using internet facilities to carry out the process of changing information. Data security is very important. The need for information makes website developers present a variety of services for users (Dharmawan et al., 2013). But most of the website developers ignore system security on the website. The most widely used attack by these attackers is the SQL Injection attack. This study focused on securing the system using the Rijndael algorithm to encrypt data (Minier, 2017). The Rijndael algorithm was chosen as a cryptographic algorithm that can protect information well and efficiently in its implementation and was named the Advanced Encryption Standard (Daemen and Rijmen, 1998; Daemen and Rijmen, 2013). This algorithm will be embedded in the system login to protect unauthorized access from the attacker (Dawood and Hammadi, 2017; Sajadieh et al., 2017). The results of using the Rijndael algorithm can protect the login system properly so that the system is declared safe from the attackers (Kuo and Verbauwhede, 2001).

Computer network security is part of a system that is very important to maintain data validity and integrity and ensure availability of services for its users (Arta et al., 2016). The current network intruder detection system is generally able to detect various attacks but is unable to take further action. But on the one hand, hu-mans are very dependent on information systems. This has caused the statistics of network security incidents to continue to increase sharply from year to year (Namjoshi and Narlikar, 2014; Waisman et al., 2007). This is due to the people's lack of concern for network security systems. We need a system that can help network administrators to be used as a network traffic monitor with Intrusion Prevention System (IPS) which is a combination of blocking capabilities from Firewall (Giokas, 2016).

Arta, Y., Pratama, H., Siswanto, A., Syukur, A. and Setiawan, P.
Design of Web Login Security System using ElGamal Cryptography.
DOI: 10.5220/0009186802680273
In *Proceedings of the Second International Conference on Science, Engineering and Technology (ICoSET 2019)*, pages 268-273
ISBN: 978-989-758-463-3

2 ElGamal ENCRYPTION

The process of key formation is the process of determining a number which will then be used as a key in the process of encryption and decryption of messages(Hashim, 2014). The key for encryption is generated from the p value, g, y while the decryption key consists of the value x, p (Makkaoui et al., 2016). each value has requirements that must be met. Rare in making keys are as follows:

- Primes p, with p values $>$ 255.
- Select a random number g with the condition g $<$ p.
- Select a random number x with the condition 1 $<$ x $<$ p-2.
- Calculate y = g * x mod p.

The public key is y, g, p while the private key is x. the value of y, g, and p is not save secret while the value of x must be kept secret because it is a private key to describe plaintext (Kiltz and Pietrzak, 2010; Tsiounis and Yung, 1998; Weinberger et al., 2006).

3 RESULT AND DISCUSSION

3.1 Username Encryption Process with ElGamal Algorithm

In this section a comparison will be made between the ElGamal login username and the standard login on the web login system using ElGamal cryptography, the results of the comparison can be seen in table 1.

The process in table 1 above, is the result of the encryption process using the ElGamal method. Below this is the process of an ElGamal method at work.

- If the testing system uses a username: 23081990, Number of characters: 59, Uppercase: 0, Small letters: 0, Numbers: 8, special character: 0, Other: 15, Results: 8.81.
- If the testing system uses username: abcd1234, Number of characters: 58, Uppercase: 0, Small letters: 4, Numbers: 8 special character: 0, Other: 15, Result: 4,058.
- If the testing system uses username: AbCd1234, Number of characters: 56, Upper-case: 2, Small letters: 2, Numbers: 4, special character: 0, Other: 15, Result: 4,058.
- If the test system uses a username: Ac54$# h, Number of characters: 50, Uppercase: 1, Small letter: 2, Numbers: 2, Special character: 2, Other: 13, Result: 23,941.
- If the testing system uses a username: 6$ Ab788, Number of characters: 50, Uppercase: 1, Small letter: 1, Number: 3, Special character: 1, Other: 13, Result: 19.981.
- If the test system uses username: aaD#6754, Number of characters: 57, Uppercase: 1, Small letter: 2, Number: 4, special character: 1, Other: 15, Result: 4,995.
- If the testing system uses username: &*$# 9764, Number of characters: 59, Uppercase: 0, Small letters: 0, Number: 4, Special character: 4, Other: 15, Result: 9,313.

The process in table 2 above, is the result of the encryption process using the standart character. Below this is the process of standard login process testing

- If the test system uses a username: 23081990, Number of characters: 8, Large letters: 0, Lower case letters: 0, Numbers: 8, character specials: 0, Other: 0 Result: 0.
- If the testing system uses username: abcd1234, Number of characters: 8, Large letters: 0, Lowercase letters: 4, Numbers: 8, Special characters: 0, Other: 0, Results: 0.13.
- If the testing system uses username: AbCd1234, Number of characters: 8, Large letters: 2, Lowercase letters: 2, Numbers: 4, Special characters: 0, Other: 0, Results: 0.13.
- If the testing system uses a username: Ac54$#h, Number of characters: 7, Large letters: 1, Lowercase: 2, numbers: 2, special character: 2, Other: 0, Results: 0.5.
- If the testing system uses a username: 6$Ab788, Number of characters: 7, Large letters: 1, Lowercase: 1, Number: 3, Special characters: 1, Other: 0, Result: 0.2.
- If the testing system uses username: aaD#6754, Number of characters: 8, Large letters: 1, Lowercase: 2, Number: 4, Special character: 1, Other: 0, Results: 0.16.
- If the testing system uses username: &*$# 9764, Number of characters: 8 ,Large letters: 0, Lower case letters: 0, Numbers: 4, special character: 4, Other: 0, Results: 0.31.

In table 1 dan 2 above can be seen the comparison between the ElGamal login username and the standard login that has been done. Then the comparison results will be accumulated into a graph and can be seen in figure 1.

In Figure 1, the average time of the encryption and decryption results of each username gets an ElGamal

Table 1: Username for ElGamal Login Testing.

ElGamal								
Exam	Username	Char Encryp	char(U)	Char(L)	Number	Special(A)	Other	Result
1	23081990	59	0	0	8	0	15	8.81
2	abcd1234	58		4	4	0	15	4.05
3	AbCd1234	56	2	2	4	0	15	4.05
4	Ac54$#h	50	2	1	2	2	13	23.9
5	6$Ab788	50	1	2	3	1	13	19.9
6	aaD#6754	57	1	2	4	1	15	4.99
7	&*$#9764	59	0	0	4	4	15	9.31

Table 2: Username for Standard Login Testing.

Standard								
Exam	Username	Char Encryp	char(U)	Char(L)	Number	Special(A)	Other	Result
1	23081990	8		0	8		0	0
2	abcd1234	8		4	4		0	0.13
3	AbCd1234	8	2	2	4		0	0.13
4	Ac54$#h	7	2	1	2	2	0	0.5
5	6$Ab788	7	1	2	3	1	0	0.2
6	aaD#6754	8	1	2	4	1	0	0.16
7	&*$#9764	8	0	0	4	4	0	0.31

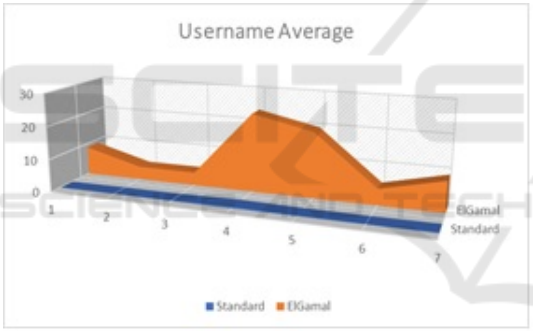

Figure 1: Username Average (Second).

value: 27, 87 and standard: 0.2. Processing requires a longer span of time than the standard username because each process from ElGamal requires the insertion of a value before entering the username.

3.2 Password Encryption Process with ElGamal Algorithm

In this section a comparison will be made between the ElGamal login password and the standard login on the web login system using ElGamal cryptography, the results of the comparison can be seen in table 3.

When a password is given a character using standard letters, the time required does not take a long process of about 13 seconds. For ElGamal use using ASCII numbers, it will take quite a long time. The combination of standard letters and also ASCII numbers is a safe step.

Password ElGamal Process Testing

- If the testing system uses a username: kauy984, number of characters: 51, uppercase: 3, lowercase: 1, number: 3, special characters: 0, other: 13, Result: 16,235.
- If the test system uses username: abdx*&#, number of characters: 53, uppercase: 2, lowercase: 2, numbers: 0, special characters: 3, other: 13, Results: 53.99.
- If the testing system uses username: abcd1234, number of characters: 56, uppercase: 2, lowercase: 2, numbers: 4, character specials: 0, other: 15, Results: 4,058.
- If the testing system uses a username: 65*&%̂k, number of characters: 53, uppercase: 0, lowercase: 1, number: 2, special characters :4, other: 13, Results: 63,941.
- If the test system uses username: 6$ab788, number of characters: 50, uppercase: 1, lowercase: 1, number: 3, special characters: 1, other: 13, results: 19.981.
- If the test system uses username: aad#6754, number of characters: 57, uppercase: 1, lowercase :2, number: 4, special characters: 1, other: 15, Results: 4.995.
- If the test system uses username: &*$# 9764, number of characters: 59, uppercase: 0, lower-

Table 3: Password for ElGamal Login Testing.

ElGamal								
Exam	Password	Char Encryp	char(U)	Char(L)	Number	Special(A)	Other	Result
1	kAUY984	51	3	1	3		13	16.2
2	abDX*&#	53	2	2	0	3	15	53.9
3	AbCd1234	56	2	2	4		15	4.05
4	65*&^%k	53	0	1	2	4	13	63.9
5	6$Ab788	50	1	2	3	1	13	19.9
6	aaD#6754	57	1	2	4	1	15	4.99
7	&*$#9764	59	0	0	4	4	15	9.31

case: 0, number: 4, special characters: 4, other: 15, Results: 9,313.

The results from table 4 that use standard numbers, are not much different from previous experiments. And for the average results of the above test is 0.23 seconds.

Standart Password Process Testing

- If the test system uses username: kauy984, number of characters: 7, uppercase letters: 4, lowercase letters: 0, numbers: 3, character specials: 0, other: 0, Results: 0.01.
- If the testing system uses username: abdx*&#, number of characters: 7, uppercase: 2, lowercase: 2, numbers: 0, special characters: 3, other: 0, Results: 0.44.
- If the test system uses username: abcd1234, number of characters: 8, uppercase: 2, lowercase: 2, numbers: 4, special characters: 0, other: 0, Results: 0.13.
- If the test system uses a username: 65*&*%k, number of characters: 7, uppercase: 0, lowercase: 1, number: 2, special characters: 4, other: 0, results: 0.4.
- If the testing system uses a username: 6$ ab788, number of characters: 8, uppercase: 1, lowercase: 1, number: 3, special characters: 1, other: 0, Result: 0.2.
- If the test system uses username: aad#6754, number of characters: 8, uppercase: 1, lowercase: 2, number: 4, special characters: 1, other: 0, Result: 0.16.
- If the test system uses username: &*$# 9764, number of characters: 8, uppercase letters: 0, lowercase letters: 0, numbers: 4, character specials: 4, other: 0, Results: 0.31.

In table 2 above can be seen the comparison between the ElGamal login username and the standard login that has been done. Then the comparison results will be accumulated into a graph and can be seen in figure 2.

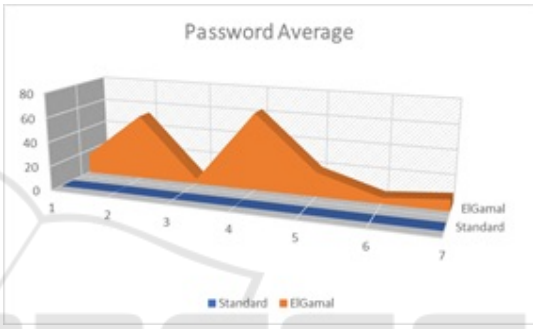

Figure 2: Password Average (Second).

In Figure 2, it can be seen that the process of inserting a value into a password takes time. This value is used for comparison when a password is to be tested if it is security, it will take a longer time than just using a password that does not use ElGamal. This is a subjective assessment for a password security trial. for the average process of a password using the ElGamal method and ASCII numbers, it takes 24.64 seconds.

The following is the comparative result of calculations based on ElGamal and Standard login. To increase the security of the username and password on the ElGamal encryption login, it should be added to the length of the character, because the more the length of characters, the more difficult the hackers intend to break into ElGamal encryption login system. The graph of these methods are shown in figure 3.

4 CONCLUSIONS

From the comparison test results above, it can be concluded that the level of security and average hourly for comparison testing Elgamal login username: 10.73 and for testing the comparison of standard login username: 0.20. Then for testing the comparison of Elga-

Table 4: Password for Standart Login Testing.

Standard								
Exam	Password	Char Encryp	char(U)	Char(L)	Number	Special(A)	Other	Result
1	kAUY984	7	3	1	3		0	0.01
2	abDX*&#	7	2	2	0	3	0	0.44
3	AbCd1234	8	2	2	4		0	0.13
4	65*&^%k	7	0	1	2	4	0	0.4
5	6$Ab788	7	1	2	3	1	0	0.2
6	aaD#6754	8	1	2	4	1	0	0.16
7	&*$#9764	8	0	0	4	4	0	0.31

Table 5: Comparison of Username Password.

USERNAME	ElGamal	Standard	PASSWORD	ElGamal	Standard
23081990	8.81	0	kAUY984	16.235	0.01
abcd1234	4.058	0.13	abDX*&#	531.99	0.44
AbCd1234	4.058	0.13	AbCd1234	4.058	0.13
Ac54$#h	63.941	0.5	65*&^%k	63.941	0.4
6$Ab788	19.981	0.2	6$Ab788	19.981	0.2
aaD#6754	4.995	0.16	aaD#6754	4.995	0.16
&*$#9764	9.313	0.31	&*$#9764	9.313	0.31
Average	10.73	0.20	Average	24.64	0.23

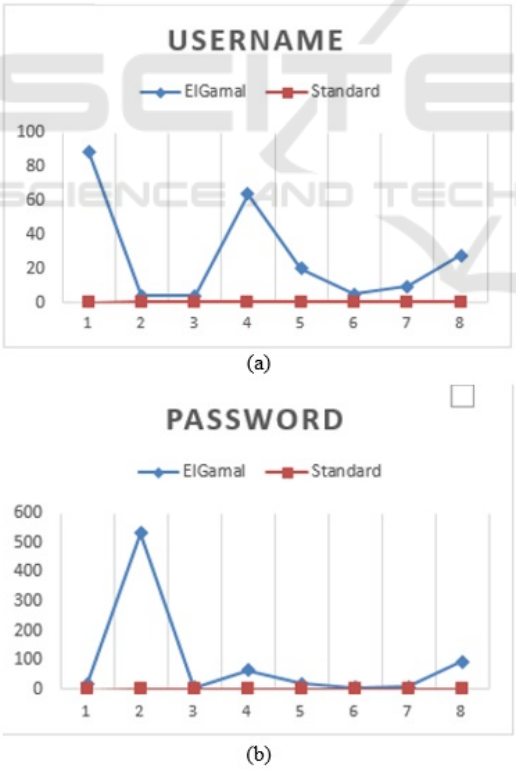

Figure 3: Graph Comparison ElGamal And Standard Login (a) Top and (b) bottom views.

mal login passwords: 24.64 and for testing the comparison of standard login passwords: 0.23.

ACKNOWLEDGEMENTS

We would like to express our gratitude to the Universitas Islam Riau for the fund this project.

REFERENCES

Arta, Y. (2017). Implementasi intrusion detection system pada rule based system menggunakan sniffer mode pada jaringan lokal. *IT Journal Research and Development*, 2(1):43–50.

Arta, Y., Kadir, E. A., and Suryani, D. (2016). Knoppix: Parallel computer design and results comparison speed analysis used amdahl theory. In *2016 4th International Conference on Information and Communication Technology (ICoICT)*, pages 1–5. IEEE.

Arta, Y., Syukur, A., and Kharisma, R. (2018). Simulasi implementasi intrusion prevention system (ips) pada router mikrotik. *IT JOURNAL RESEARCH AND DEVELOPMENT*, 3(1):104–114.

Daemen, J. and Rijmen, V. (1998). The block cipher Rijndael. In *International Conference on Smart Card Research and Advanced Applications*, pages 277–284.

Daemen, J. and Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media.

Dawood, O. A. and Hammadi, O. I. (2017). An analytical study for some drawbacks and weakness points

of the AES cipher (rijndael algorithm). In *The 1 st International Conference on Information Technology (ICoIT17)*, page 126.

Dharmawan, E. A., Yudaningtyas, E., and Sarosa, M. (2013). Perlindungan Web pada Login Sistem Menggunakan Algoritma Rijndael. *Jurnal EECCIS*, 7(1):77–84.

Giokas, I. (2016). *April 19)*. Systems and methods for self-tuning network intrusion detection and prevention.

Kiltz, E. and Pietrzak, K. (2010). Leakage resilient elgamal encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 595–612.

Kuo, H. and Verbauwhede, I. (2001). *Architectural optimization for a 1*. 82 Gbits/sec VLSI implementation of the AES Rijndael algorithm.

Makkaoui, E., K., B.-H., A., and Ezzati, A. (2016). Cloud-ElGamal: An efficient homomorphic encryption scheme. In *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pages 63–66.

Minier, M. (2017). Improving impossible-differential attacks against Rijndael-160 and Rijndael-224. *Designs, Codes and Cryptography*, pages 117–129.

Namjoshi, K. S. and Narlikar, G. J. (2014). *March 25)*. Method and apparatus for pattern matching for intrusion detection/prevention systems.

Novendra, Y., Arta, Y., and Siswanto, A. (2018). Analisis perbandingan kinerja routing ospf dan eigrp. *IT JOURNAL RESEARCH AND DEVELOPMENT*, 2(2):97–106.

Sajadieh, M., Mirzaei, A., Mala, H., and Rijmen, V. (2017). A new counting method to bound the number of active S-boxes in Rijndael and 3D. *Designs, Codes and Cryptography*, 83(2):327–343.

Tsiounis, Y. and Yung, M. (1998). On the security of ElGamal based encryption. In *International Workshop on Public Key Cryptography*, pages 117–134.

Waisman, N., Paterno, H. A., Mata, C. L., and Tamaroff, A. R. (2007). *May 29)*. Methods and apparatus for computer network security using intrusion detection and prevention.

Weinberger, K. Q., Blitzer, J., and Saul, L. K. (2006). Distance metric learning for large margin nearest neighbor classification. In *Advances in neural information processing systems*, pages 1473–1480.