© 2018 IJSRST | Volume 4 | Issue 10 | Print ISSN : 2395-6011 | Online ISSN : 2395-602X
Themed Section: Science and Technology

Three-Pass Protocol Scheme using Gronsfeld and Vigenere Ciphers

Ranti Eka Putri, Andysah Putera Utama Siahaan
Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia

ABSTRACT

Classical cryptographic algorithms are algorithms that can help users to process encryption and decryption efficiently. Because it is easy, this algorithm is often hacked by wild parties. This algorithm has the power that is vulnerable to attacks on keys. The key used can be hijacked, and finally, the ciphertext can be solved. The plaintext can eventually be found because the key has been taken. The combination of two classical algorithms using the Three-pass Protocol scheme is beneficial because the information sent is stronger because this process does not distribute the key to the recipient of the information. Each actor will do encryption and decryption with their keys. The key will not be exchanged, and the key does not need to be known by the sender and recipient. This scheme is very safe to use because there are no key shipments through the global network. The Three-pass Protocol concept creates a power that is far better than the usual classical cryptographic process.

Keywords : Three-Pass Protocol, Gronsfeld, Vigenere, Encryption, Decryption, Algorithm

I. INTRODUCTION

The global network in the world of computers is currently the best target for people who intend to do cybercrime. The global network will be connected to each small system where everyone can access and conduct security testing on the network. Some try to increase security, and some try to commit crimes [1]. A computer network is a system consisting of several computers designed to be able to share hardware and share data. Therefore computer networks also need guaranteed security to avoid data hackers. Network security itself is a process that is useful to prevent and analyze unauthorized use of computer networks both locally and globally [2]. Preventive measures are beneficial to stop wild parties from accessing any part of a computer network system. Cryptography is needed in a network system to protect data when connected to a global network. It is also done when sending data; cryptography will secure the information that is being sent [3].

Cryptography is an algorithm for converting information from its original form into an incomprehensible form [4]. Someone who knows the password can only reopen ciphertext. Because it guarantees the security of users, cryptography is very useful for hiding and securing user files. User reasons for hiding files can be various. One of them, there are those who need cryptography for privacy reasons and the private interests of users, some are doing it because it contains state information and military strategies. So that with this cryptography, users do not need to worry or fear if their privacy will be uncovered [5]–[8]. Cryptography is also used for authentication reasons where the recipient of the message can ensure that the information obtained remains original and unmodified. Message recipients do not need to worry if the message sent is a message

that comes from the owner. It greatly facilitates the use of exchanging information freely. This method is also used during wars so that information is not leaked to enemy areas. However, cryptography does not guarantee the security of information in its entirety. There is still a possibility where hackers try to break the piece of information they get. The chance of success to crack passwords still exists. How long the message breaks depends on the strength of a cryptographic algorithm [9]. Seeing computer security increasingly threatened, a method is needed that can anticipate this error. The Three-pass Protocol method is a feasible technique to be used to increase the level of security on the network. This method avoids key exchanges on the sender and recipient of information. This method is expected to be very helpful for users to carry out activities on the global network safely and peacefully.

II. THEORIES

2.1 Importance of Computer and Network Security

Not only protects the hard and soft devices of the company, but the most important thing is to protect the information held by the company. Because data is something that is very valuable, the owner must protect that [10]. Developing and maintaining network security in a company helps the company maintain and enhance the reputation of the company in an increasingly tight competition. Network security is essential in financial services via the internet or eCommerce. The safer protection of network services will increase consumer confidence in the company. Example: what happens if a bank customer knows how bad the security level of the bank e-banking service is. The customer will move to another bank whose e-banking security level is better than that of the bank. The company's performance will significantly increase with good network security. Employee performance becomes disrupted in serving customers if the network is in trouble. The customer becomes anxious because of how long the company can provide the service. If the service is excellent, the customer is satisfied, the performance of the company will function well, and the number of customers will increase. However, on the contrary, if the performance is bad, customers will run away and move to another company. The company will suffer more losses, and eventually, the company will experience a significant loss [11].

2.2 Cryptography

Cryptography, in general, is science and art to maintain the confidentiality of news. In addition to this understanding, there is also an understanding of the knowledge of mathematical techniques relating to information security aspects such as data confidentiality, data validity, data integrity, and data authentication. Not all aspects of information security are handled by cryptography [12]. There are four fundamental goals of cryptography which are also aspects of information security 12], such as:

- Confidentiality is a service that is used to protect the contents of information from anyone except those who have the authority or secret key to open/analyze information that has been encoded.
- Data integrity is related to the maintenance of unauthorized data changes. The system must have the ability to detect data manipulation by unauthorized parties, including insertion, deletion, and subsidization of other data into the actual data.
- Authentication is related to the identification, both unity of the system and the information itself. Two parties who communicate with each other must introduce themselves. Information sent through the channel must be authenticated authenticity, data content, delivery time, and so on.
- Non-repudiation or non-denial is an attempt to prevent the denial of the creation of information by the sender.

Two processes involving cryptographic activities in conducting information security are [13]:

1. Encryption
2. Decryption

2.3 Gronsfeld Cipher

Gronsfeld Cipher is a cryptographic algorithm that works the same way as the Vigenere Cipher algorithm. The fundamental difference is that Vigenere uses alphabet to substitute plaintext while Gronsfeld uses numbers to shift the plaintext character to the key [14]. This algorithm uses 256 ASCII characters for the calculation process in the substitution table. The following equations are the formulas used to implement the Gronsfeld algorithm.

$$E(x) = (P(x) + K(x)) \bmod 256$$

$$D(x) = (P(x) - K(x)) \bmod 256$$

Addition process occurs in encryption and subtraction occurs in decryption. If the processed character exceeds 256 or more than 0, then the character will experience the modulo process to get the ciphertext or plaintext character [15].

2.3 Vigenère Cipher

Vigenère Cipher is probably the best example of a 'manual' alphabet-compound cipher. This algorithm was published by the French diplomat, Blaise de Vigènere in the 16th century. Vigènere Cipher was published in 1586. Vigènere Cipher uses Vigènere's roots to encrypt. The leftmost column of the rectangle represents the key letters, while the top row represents plaintext letters. The number of plaintext letters is determined by the numeric value of the key letter.

Vigenere is the name of the person who invented the method for creating a password. This password is not easy to solve but to make this password is also not secure. So this password is not suitable for use during scouts or during emergencies. The weakness of the Vigenère cipher algorithm appears if the key length is shorter than the length of the plaintext so that there is a loop of keys used to encrypt the plaintext. The repeated key creates a gap in the form of the same amount of shift for each plaintext that is substituted by the letter on the same key so that the letters of the message or plaintext can be grouped based on the key used. Because there is a group of plaintext letters substituted with the same key letter because of the key loop, then each group of letters can be subjected to a frequency analysis method against it. It can be known the key length using the Kasiski method. It is because there are generally repetitive phrases on the ciphertext generated.

Kasiski Testing Method is a Vigenère Cipher algorithm testing method where the function of this method is to analyze the length of the key used by a cryptanalyst in encrypting a plain text into ciphertext. The rule of this Kasiski Method is to analyze the set of series which has the most frequent occurrence index in the ciphertext. Then the set is eliminated so that the key length is likely to be used in the Vigenère Cipher algorithm encryption process [16].

III. RESULT AND DISCUSSION

This section explains the Gronsfeld algorithm testing. This algorithm is one of the classic cryptographic algorithms that use symmetrical keys. This method is straightforward to implement because this algorithm has an easy calculation. Even though the key is simple, this algorithm has a high complexity to solve if using a long key because the key loop is unpredictable in which part. The following is an illustration of the Gronsfeld algorithm calculation.

Plaintext =

P1	P2	P3	P4	P5	P6	P7	P8	P9
I	N	D	O	N	E	S	I	A

Key =

K1	K2	K3	K4	K5	K6
1	2	3	4	5	6

Plaintext ASCII =

P1	P2	P3	P4	P5	P6	P7	P8	P9
I	N	D	O	N	E	S	I	A
73	78	68	79	78	69	83	73	65

3.1 Gronsfeld Encryption

C1 = P1 + K1
= 73 + 1
= 74

C2 = P2 + K2
= 78 + 2
= 80

C3 P3 + K3
= 68 + 3
= 71

C4 = P4 + K4
= 79 + 4
= 83

C5 = P5 + K5
= 78 + 5
= 83

C6 = P6 + K6
= 69 + 6
= 75

C7 = P7 + K1
= 83 + 1
= 84

C8 = P8 + K2
= 73 + 2
= 75

C9 = P9 + K3
= 65 + 3
= 68

Ciphertext =

C1	C2	C3	C4	C5	C6	C7	C8	C9
74	80	71	83	83	75	84	75	68
J	P	G	S	S	K	T	K	D

3.2 Vigenère Encryption

Plaintext =

P1	P2	P3	P4	P5	P6	P7	P8	P9
J	P	G	S	S	K	T	K	D

Key =

K1	K2	K3	K4	K5	K6	K7	K8	K9
a	b	c	d	e	f	g	h	i
97	98	99	100	101	102	103	104	105

Ciphertext =

P1	P2	P3	P4	P5	P6	P7	P8	P9
74	80	71	83	83	75	84	75	68
J	P	G	S	S	K	T	K	D
K1	K2	K3	K4	K5	K6	K7	K8	K9
a	b	c	d	e	f	g	h	i
97	98	99	100	101	102	103	104	105
C1	C2	C3	C4	C5	C6	C7	C8	C9
171	178	170	183	184	177	187	179	173
«	²	ª	·	¸	±	»	³	

3.3 Gronsfeld Decryption

P1 = C1 - K1
= 171 - 1
= 70

P2 = C2 - K2
= 178 - 2
= 176

P3 = C3 - K3
= 170 - 3
= 167

P4 = C4 - K4
= 183 - 4
= 179

P5 = C5 - K5
= 184 - 5
= 179

P6 = C6 - K6
= 177 - 6
= 171

P7 = C7 - K1
= 187 - 1
= 186

P8 = C8 - K2
= 179 - 2
= 177

P9 = C9 - K3
= 173 - 3
= 170

Plaintext =

C1	C2	C3	C4	C5	C6	C7	C8	C9
171	178	170	183	184	177	187	179	173
«	²	ª	·	¸	±	»	³	
K1	K2	K3	K4	K5	K6	K1	K2	K3
1	2	3	4	5	6	1	2	3
P1	P2	P3	P4	P5	P6	P7	P8	P9
170	176	167	179	179	171	186	177	170
ª	°	§	³	³	«	º	±	ª

3.2 Vigenère Decryption

Ciphertext =

C1	C2	C3	C4	C5	C6	C7	C8	C9
ª	°	§	³	³	«	º	±	ª

Plaintext =

C1	C2	C3	C4	C5	C6	C7	C8	C9
170	176	167	179	179	171	186	177	170
ª	°	§	³	³	«	º	±	ª
K1	K2	K3	K4	K5	K6	K7	K8	K9
a	b	c	d	e	f	g	h	i
97	98	99	100	101	102	103	104	105
P1	P2	P3	P4	P5	P6	P7	P8	P9
73	78	68	79	78	69	83	73	65
I	N	D	O	N	E	S	I	A

IV. CONCLUSION

Cryptographic processes will be excellent if combined with other methods. Three-pass Protocol is a concept where both cryptographic actors do not need to exchange keys for providing additional security for information that is on a global network. When hackers have obtained a piece of information in the form of ciphertext, it is not confident that they can crack the password codes. It happens because the key used by the sender and recipient is not distributed to each other. No key exchanges occur in the air. The level of information security will be much better using the Three-pass Protocol scheme.

V. REFERENCES

[1] Hariyanto dan A. P. U. Siahaan, "Intrusion Detection System in Network Forensic Analysis and," IOSR J. Comput. Eng., vol. 18, no. 6, hal. 115–121, 2016.

[2] H. Ming dan S. LiZhong, "A New System Design of Network Invasion Forensics," in 2009 Second International Conference on Computer and Electrical Engineering, 2009, hal. 596–599.

[3] F. Azzuhry, "Manfaat Kriptografi dalam Kehidupan," UGM, 2012. [Daring]. Tersedia pada: http://fattah-azzuhry.blog.ugm.ac.id/2012/02/23/manfaat-kriptografi-dalam-kehidupan/.

[4] V. Tasril, M. B. Ginting, Mardiana, dan A. P. U. Siahaan, "Threats of Computer System and its Prevention," Int. J. Sci. Res. Sci. Technol., vol. 3, no. 6, hal. 448–451, 2017.

[5] A. P. U. Siahaan, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," Int. J. Adv. Appl. Sci., vol. 6, no. 4, hal. 313–318, 2017.

[6] A. P. U. Siahaan, "Genetic Algorithm in Hill Cipher Encryption," Am. Int. J. Res. Sci. Technol. Eng. Math., vol. 15, no. 1, hal. 84–89, 2016.

[7] I. Sumartono, A. P. U. Siahaan, dan N. Mayasari, "An Overview of the RC4 Algorithm," IOSR J. Comput. Eng., vol. 18, no. 6, hal. 67–73, 2016.

[8] I. Sumartono, A. P. U. Siahaan, dan Arpan, "Base64 Character Encoding and Decoding Modeling," Int. J. Recent Trends Eng. Res., vol. 2, no. 12, hal. 63–68, 2016.

[9] A. Lubis dan A. P. U. Siahaan, "Network Forensic Application in General Cases," IOSR J. Comput. Eng., vol. 18, no. 6, hal. 41–44, 2016.

[10] W. Stallings, Cryptography and Network Security: Principles and Practice. New Jersey: Prentice Hall Press, 2013.

[11] M. Abror, "Pengertian dan Aspek-Aspek Keamanan Komputer," 2018. [Daring]. Tersedia pada: https://www.ayoksinau.com/pengertian-dan-aspek-aspek-keamanan-komputer-lengkap/. [Diakses: 01-Okt-2018].

[12] A. . Paul, P. Mythili, dan K. Paulose Jacob, "Matrix based cryptographic procedure for efficient image encryption," in 2011 IEEE Recent Advances in Intelligent Computational Systems, 2011, hal. 173–177.

[13] J. A. Buchmann, Introduction to Cryptography, 1st ed. Berlin: Springer-Verlag, 2000.

[14] Mesran, "Gronsfeld Cipher," Wordpress, 2011. [Daring]. Tersedia pada: https://mesran.wordpress.com/2011/07/03/gronsfeld-cipher/. [Diakses: 01-Okt-2018].

[15] D. Apriadi, "Kriptografi Kunci Simetris Gronsfeld Chiper," Blogspot, 2016. [Daring]. Tersedia pada: https://dodi-apriadi.blogspot.com/2016/02/kriptografi-kunci-simetris-gronsfeld.html. [Diakses: 01-Okt-2018].

[16] G. M. Pratama dan E. N. Tamatjita, "MODIFIKASI ALGORITMA VIGENERE CIPHER MENGGUNAKAN METODE CATALAN NUMBER DAN DOUBLE COLUMNAR TRANSPOSITION," Compiler, vol. 4, no. 1, hal. 31–40, 2015.