Journal of Critical Reviews
ISSN- 2394-5125 Vol 7, Issue 1, 2020

Three-pass Protocol Scheme on Vigenere Cipher to Avoid Key Distribution

Khasanah[1], Phong Thanh Nguyen[2*], G Gunawan[3], Robbi Rahim[4]

[1]STMIK Indonesia Jakarta, Jakarta, Indonesia. Email: khasanah.pase@gmail.com
[2]Department of Project Management, Ho Chi Minh City Open University, Vietnam. Email: phong.nt@ou.edu.vn
[3]Department of Physics Education, Universitas Mataram, Indonesia
[4]Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia. Email: usurobbi85@zoho.com

Received: 09.10.2019 Revised: 10.11.2019 Accepted: 11.12.2019

Abstract:
Information exchange is a prevalent thing in computer networks. The information sent is confidential, and some are ordinary. In sending confidential information, many concerns occur. The sender is afraid of the information being stolen, especially if the information contains confidential data. In sending information, the sender and recipient must know the key or password to be able to read the information correctly. However, sending the key is very deep concern because if others know the key, then the data and information contained in the file will be successfully read. Key exchanges must be avoided. The technique for avoiding key exchange is to use the Three-pass Protocol scheme. This scheme allows the sender and receiver to encrypt and decrypt using their respective keys without having to exchange keys. Three-pass Protocol is a mechanism. There are two algorithms needed in the cryptographic process. The algorithm used is Vigenere Cipher. By implementing the Three-pass Protocol scheme, data security will be more guaranteed.

***Key Words**:* three-pass protocol, encryption, decryption, Vigenere

 DOI: http://dx.doi.org/10.22159/jcr.07.01.13

INTRODUCTION

Exchange of information is the most often done thing. The exchange of information occurs because the sender and receiver of the data are not in the same location, so that requires an exchange of data through a computer network [1]. Information is a message that will be delivered to the recipient for certain things. Sometimes, this information contains a secret message so that others cannot know it. In sending information, many things must be performed. The essential components is data security. The data or information must reach the recipient without any interruption in his journey. However, this will be not very easy to avoid. The most significant opportunity is to encrypt data and not give keys to recipients through computer networks to avoid theft and misuse of information [2].

There is a technique to avoid key exchanges so that the information sent is only encrypted messages. This technique is called the Three-pass Protocol. This technique allows the sender and receiver to use their respective keys in the encryption and decryption process. The sender and receiver can use their respective keys without having to tell each other the contents of the key so that this key is entirely safe and does not leak. The key has never been sent or reported through the internet [3].

The Three-pass Protocol scheme requires the sender and receiver to continue the encryption process. The difference is that the recipient continues the encryption process; this is different from the scheme without the Three-pass Protocol, where the recipient only decrypts. The Three-pass Protocol process can use the same cryptographic algorithm in both processes or use different algorithms in the sender and receiver encryption processes. The algorithm used in the Three-pass Protocol scheme is a classic algorithm so that the calculation process at the time of encryption and decryption is more straightforward. The advantage of classical algorithms is that the cryptographic process will be faster because of its simple computation without involving many mathematical calculations [4].

THEORIES

2.1 Three-pass Protocol

Three-pass Protocol is a concept of sending information that let the sender to send messages securely to receiver using its key and the receiver decrypt the encrypted messages using its key as well. The do not need to exchange or distribute the key provided in the encryption or decryption. The message technique should not be distracted with a variety of other algorithms that use three passes for verification [5], [6].

The name of the technique is three pass protocol. It is called because of the sender and receiver preform three ciphertext. Judging from the way it works, the concept of the Three-pass Protocol does not require password exchange in the cryptographic process. There are two participants involved in the Three-pass Protocol process. The sender will send a series of data that was previously encrypted using an algorithm. The algorithm used is the classic cryptographic algorithm. The recipient will receive the results of encryption from the sender that was previously encrypted with the agreed algorithm. The receiver will then re-encrypt the same algorithm or another algorithm that matches the Three-pass Protocol scheme. After the message is encrypted, the message produces a second ciphertext. This ciphertext will be sent back to the sender. The sender receives a message that has been encrypted twice. The sender decrypts the message using the sender's key. The decryption result is the third ciphertext. The message is finally sent back to the recipient. The recipient will decrypt the last of the third ciphertext. The decryption results are plaintext that can be read and understood by the recipient. The recipient and sender do not need to exchange keys so that there is no leakage of key exchange information. The concept of the Three-pass Protocol is very safe in sending messages, but the Three-pass Protocol will work by consuming twice the general concept [7] [8].

2.2 Vigenere Cipher

Vigenère Cipher is a method of encrypting the alphabet text. It uses a simple polyalphabetic substitution form. It is a cipher based on substitution, using several substitution letters [9]. The vigènere code is a polyalphabetic substitution cipher. It was published by a French diplomat (and also a cryptologist), Blaise de Vigènere in the 16th century, 1586. Giovan Batista explained it for the first time in 1533, as written in the book La Cifra del Sig. This algorithm was widely known 200 years later and was called the code vigènere. Vigènere was the trigger for civil war in America, and the Confederate Army used the vigènere code in the American Civil War. Babbage and Kasiski successfully broke the vigènere code in the mid-19th century [10]

This type of encryption algorithm is very well known because it is easy to understand and implement. The

technique to produce ciphertext can be done using number substitution or rectilinear square. The technique of substituting vigènere by using numbers is done by exchanging letters for numbers, almost the same as a sliding code [11].

METHODOLOGY

The research process involves identifying problems, finding, assessing, and analyzing the three-pass protocol process needed to support the encryption and decryption process, then developing and expressing steps in making application programs. It is is a step that is needed every time a research development is carried out. The three-pass protocol has a different way from the algorithm in general. The encryption and decryption process is done twice so that the recipient and sender do not exchange keys.

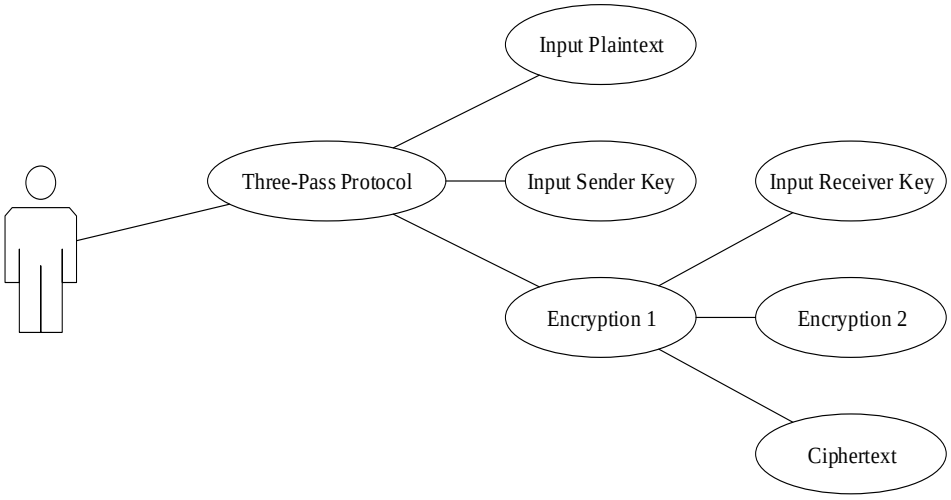

Figure 1. Encryption Process

Figure 1 is the encryption process of the sender and receiver. The sender encrypts the plaintext that has been inputted. Encryption is done using the sender's key. After becoming a ciphertext, the ciphertext will be encrypted again using the recipient key. The CIphertext will be sent back to the sender.

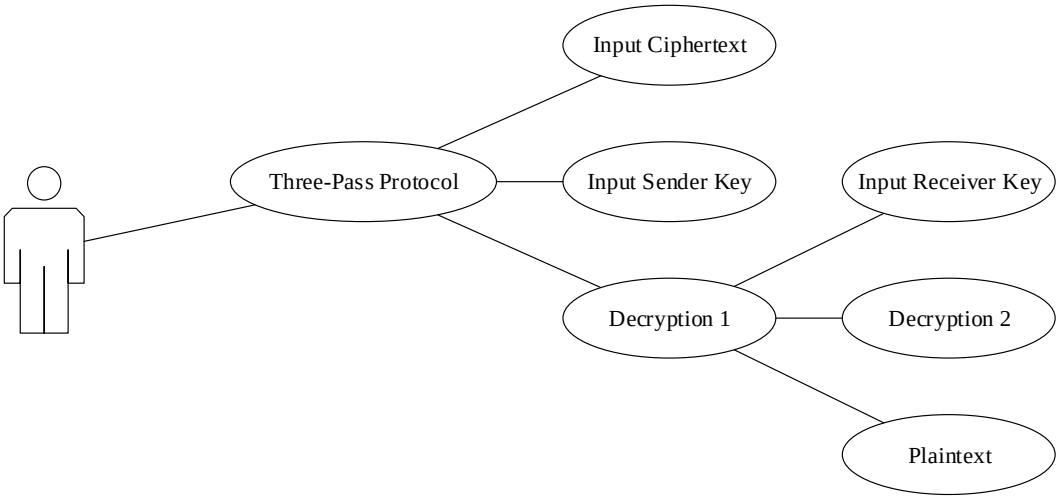

Figure 2. Decryption Process

Figure 2 is how the process of decryption and returning ciphertext into plaintext. The ciphertext that was previously sent to the sender will be decrypted using the sender's key. It will produce the last ciphertext. The ciphertext is finally received by the recipient and then decrypted to get the plaintext.

RESULT AND DISCUSSION

The following are tests conducted to determine the results of encryption and decryption using a three-pass protocol scheme. The following tables will explain how the process of transforming plaintext into ciphertext and ciphertext into plaintext.

Table 1. Encryption 1 of Vigenere Cipher

PT	ASC	KEY	ASC	ASC	CT1
R	82	I	73	155	›
A	65	N	78	143	□
I	73	D	68	141	□
N	78	O	79	157	□
N	78	N	78	156	œ
B	66	E	69	135	‡
O	79	S	83	162	¢
W	87	I	73	160	
	32	A	65	97	a
S	83	I	73	156	œ
I	73	N	78	151	—
X	88	D	68	156	œ

Table 2. Encryption 2 of Vigenere Cipher

CT2	ASC	KEY	ASC	ASC	CT2
›	155	F	70	225	á
□	143	R	82	225	á
□	141	E	69	210	Ò
□	157	E	69	226	â
œ	156	D	68	224	à
‡	135	O	79	214	Ö
¢	162	M	77	239	ï
	160	F	70	230	æ
a	97	R	82	179	³
œ	156	E	69	225	á
—	151	E	69	220	Ü
œ	156	E	69	225	á

Table 3. Decryption 1 of Vigenere Cipher

CT2	ASC	KEY	ASC	ASC	CT3
á	225	I	73	152	˜
á	225	N	78	147	“
Ò	210	D	68	142	Ž
â	226	O	79	147	“
à	224	N	78	146	’
Ö	214	E	69	145	‘
ï	239	S	83	156	œ
æ	230	I	73	157	□
³	179	A	65	114	r
á	225	I	73	152	˜

Ü	220	N	78	142	Ž
á	225	D	68	157	□

Table 4. Decryption 2 of Vigenere Cipher

CT3	ASC	KEY	ASC	ASC	PT
˜	152	F	70	82	R
“	147	R	82	65	A
Ž	142	E	69	73	I
“	147	E	69	78	N
’	146	D	68	78	N
‘	145	O	79	66	B
œ	156	M	77	79	O
□	157	F	70	87	W
r	114	R	82	32	
˜	152	E	69	83	S
Ž	142	E	69	73	I
□	157	E	69	88	X

Tables 1 and 2 are the results of plaintext encryption. Tables 3 and 4 are the decryption results of the ciphertext. The final results received by the sender are the same as those previously sent by the sender. It proves that the three-pass protocol scheme works appropriately.

CONCLUSION

Many things can be obtained from the results of research with the Three-pass Protocol scheme. The author has included several conclusions that can be drawn based on the design and implementation that has been done. The Three-pass Protocol scheme works by using two different keys in the encryption and decryption process. The sender and receiver do not need to exchange or give keys to use the Vigenere Cipher algorithm. The encryption process is done by adding ASCII plaintext 1 and ciphertext 1 values with key 1. The decryption process is done by subtracting ASCII ciphertext 2 and ciphertext 3 with keys 2. The algorithm used on the sender and receiver is the Vigenere algorithm because this algorithm is a kind of algorithm, making it easier to calculate the Three-pass Protocol scheme.

REFERENCES

1. Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, “Data Security and Privacy in Cloud Computing,” *Int. J. Distrib. Sens. Networks*, vol. 10, no. 7, p. 190903, Jul. 2014.
2. W. Stallings, *Cryptography and Network Security: Principles and Practice*. New Jersey: Prentice Hall Press, 2013.
3. R. Munir, *Kriptografi*. Bandung: Informatika, 2006.
4. Shashank, “What is Cryptography? – An Introduction to Cryptographic Algorithms,” *Edureka*, 2019. .
5. A. J. Menezes, J. Katz, P. C. van Oorschot, and S. A. Vansto, *Handbook of Applied Cryptography*. United States: CRC Press, 1996.
6. R. Rahim, “APPLIED POHLIG-HELLMAN ALGORITHM IN THREE-PASS,” *J. Appl. Eng. Sci.*, vol. 16, no. 3, pp. 424–429, 2018.
7. D. Rachmawati and M. A. Budiman, “An implementation of the H-rabin algorithm in the shamir three-pass protocol,” in *2017 2nd International Conference on Automation, Cognitive Science, Optics, Micro Electro--Mechanical System, and Information Technology (ICACOMIT)*, 2017, pp. 28–33.
8. N. Ferguson, *Cryptography Engineering: Design Principles and Practical Application*. New Jersey: Wiley Publishing, Inc., 2010.
9. A. Hidayat, “Algoritma Kriptografi Vigenere Cipher,” 2012. .
10. D. Ariyus, *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Yogyakarta: Andi Offset, 2008.
11. G. M. Pratama and E. N. Tamatjita, “MODIFIKASI ALGORITMA VIGENERE CIPHER MENGGUNAKAN METODE CATALAN NUMBER DAN DOUBLE COLUMNAR TRANSPOSITION,” *Compiler*, vol. 4, no. 1, pp. 31–40, 2015.