IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. III (Jul.-Aug. 2016), PP 26-29
www.iosrjournals.org

Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography

Boni Oktaviana[1], Andysah Putera Utama Siahaan[2]
[1]*Faculty of EngineeringSekolah Tinggi Teknik Harapan*
[2]*Faculty of Computer ScienceUniversitas Pembangunan Panca Budi*

Abstract: *This study combines classic and modern cryptographic algorithms so that the data security of information more awake authenticity. Caesar cipher is the oldest classical cryptography which uses a symmetric key method is the key used for encryption is the same as the key used for the decryption process. Three-Pass Protocol is one of the modern cryptography where the process of sending a message does not need to distribute the key so that each party both the recipient and sender of the message does not need to know each lock. In this combination of receiving and sending messages using the Caesar Cipher algorithm for encryption and decryption, while for its delivery process using algorithms Three Pass protocol. The results from the combination of the two algorithms are to help the information sent is secure.*
Keywords : *Security, Caesar Cipher, Three-Pass Protocol, Encryption, Decryption*

I. Introduction

Security of data is needed in the process of sending messages [1]; cryptographic security is one of the frequently used data. Cryptography can be divided into two parts, classic and modern cryptography [4]. Three-Pass Protocol is a modern method cryptography. The basic concept of the Three-Pass Protocol is that each party has a private encryption key and a private decryption key [2]. The shipper does not have to share a key to the recipient. Classical cryptography is an algorithm that uses a key for secure data and the process is very easy to use [7]. However,it is already old fashioned because it is considered weak in data security.

The oldest classical cryptography is the Caesar Cipher, where the Caesar Cipher algorithm that is by changing the position of the initial letter of the alphabet or also called ROT algorithm [3]. Of these problems, the main goal is to strengthen the security of the data is used in combination Caesar Cipher algorithm for encryption and decryption algorithms while three-pass protocol used to send process. The benefits of this research are that we can send messages without sharing encryption keys with other parties and strengthen Caesar Cipher algorithm in the process of sending messages.

II. Theories

The theories cover to two encryption algorithms, such as Caesar Cipher and Three-Pass Protocol. But, Three-Pass Protocol is a technique on how to make the same algorithm runs twice in encryption and decryption process. It never shares the password to both of them.

2.1 Caesar Cipher

Caesar Cipher is one the oldest and most known in the development of cryptography [6]. Caesar cipher is a substitution cipher types that make up the cipher by way of exchange of characters in plaintext into exactly one character in the ciphertext. This technique is also known as a single cipher alphabet. Caesar Cipher cryptography algorithm is very easy to use. The core of these cryptographic algorithms is shifting towards all the characters in plaintext with the same shift value. The steps taken to establish ciphertext with Caesar Cipher is:

- Determine the magnitude of the shift characters used in forming the ciphertext to plaintext.
- Redeeming the characters in plaintext into ciphertext with based on a predetermined shift.

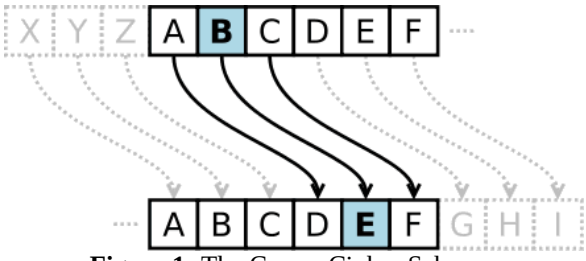

Figure 1 : The Caesar Cipher Scheme

Figure 1 shows the example of predetermined shift. In the picture, we can see every single character is moved three times from the origin. For the example, the character B, the second position in the character table, is transferred to the next characters. B moves to E. If we find this character in the encryption process, it is automatically changed to new character placed next three characters from the first one.

2.2 Three-Pass Protocol

The framework of a three-pass protocol that allows one party to send messages securely to a second party without having to exchange or distribute encryption keys. It is called a three-pass protocol for the exchange three times to authenticate the sender and recipient of the first protocol. This protocol may be realized by utilizing exclusive-OR (XOR) operations [5]. It is developed by Adi Shamir developed around 1980, the basic concept of the Three-Pass Protocol is that each party has the encryption key or a private key and a private decryption. Both sides independently using the key, to encrypt messages first, and then to decrypt the message.This protocol works in commutative ciphers or LIFO method. Commutative means that the order of encryption and decryption is interchangeable (Encryption A - Encryption B - Decryption A - Decryption B) [8]. Figure 2illustrates the Three-Pass Protocol scheme.

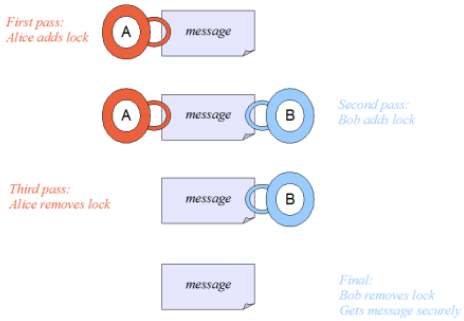

Fig. 1 : The Three-Pass Protocol scheme

III. Proposed Work

The purpose of this study, which can make the process of security to the message to be sent using different algorithms and both parties do not need to know the key to each party. In the process of encryption and decryption algorithms using Caesar Cipher. In the encoding process results obtained in the form of ciphertext. Encryption will be done twice in a row by the shipper and receiver of the message using the Caesar Cipher algorithm, as well as the decryption process performed twice in succession by the receiver and sender of the message.

The attributes used is text messages It is processed through the encryption and decryption process. There are three stages in the process of encryption and decryption of the message. The text used in this study consisted of uppercase and lowercase letters, numbers 0 through 9 and two special characters such as space and period. In this combination process using a Caesar Cipher algorithm to perform encryption and decryption of messages to be sent, while for the message delivery process using three pass algorithm protocol. A flowchart in Figure 2 is explaining the user interface, a process key generation, encryption, and decryption process in a simulation program.

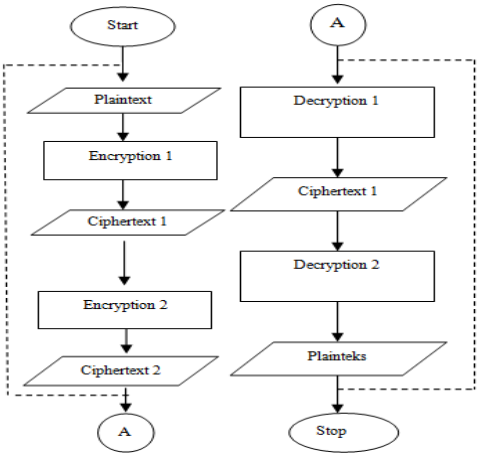

Figure 2 : Three-Pass Protocol Flow Chart

In the first stage of the encryption, the plaintext is encrypted into ciphertext. The ciphertext can not be read by unauthorized people since they do not know encryption key. The result of the encryption process is sent to the receiver without distributing the encryption key. Once the recipient receives the message in the form the sender, they will encrypt the message by using the same algorithm and send it back to the sender.And so the decryption process. The sender and receiver are using the exact keys to decrypt the message back and sent to each participant. Recipient of the message does the decryption process back to obtain the plaintext.

IV. Testing and Implementation

Now we try to prove the Three-Pass Protocol algorithm works on Caesar Cipher. We put an incoming text "REMEMBER THE PRIVATE PASSWORD" as the plaintext. The shift value is 5. The encryption process takes two times. The first, the sender must encrypt the message. After the message has arrived at the receiver, they must encrypt the message for second times. Let's see the illustration in Table 1.

Table 1 : The first round of encryption

ENCRYPTION 1								
PT	R	E	M	E	M	B	E	R
CT	W	J	R	J	R	G	J	W
PT	T	H	E					
CT	Y	M	J					
PT	P	R	I	V	A	T	E	
CT	U	W	N	A	F	Y	J	
PT	P	A	S	S	W	O	R	D
CT	U	F	X	X	B	T	W	I

In Table 1 we see the incoming text will be encrypted using Caesar Cipher. And the encryption process produces “WJRJRGJW YMJ UWNAFYJ UFXXBTWI” as the ciphertext.

Table 2 : The last round of encryption

ENCRYPTION 2								
PT	W	J	R	J	R	G	J	W
CT	A	N	V	N	V	K	N	A
PT	Y	M	J					
CT	C	Q	N					
PT	U	W	N	A	F	Y	J	
CT	Y	A	R	E	J	C	N	
PT	U	F	X	X	B	T	W	I
CT	Y	J	B	B	F	X	A	M

Table 2 shows the second round of the encryption using shift value 4. The final ciphertext would be “ANVNVKNA CQN YAREJCN YJBBFXAM”. It is the last set of the encryption process. To read the message, the participants must decrypt the final ciphertext twice.

Table 3 : The first round of decryption

DECRYPTION 1								
PT	A	N	V	N	V	K	N	A
CT	V	I	Q	I	Q	F	I	V
PT	C	Q	N					
CT	X	L	I					
PT	Y	A	R	E	J	C	N	
CT	T	V	M	Z	E	X	I	
PT	Y	J	B	B	F	X	A	M
CT	T	E	W	W	A	S	V	H

Table 3 shows the first decryption. It still produces the ciphertext format since the text is unreadable. This ciphertext needs to be sent to the receiver once again to make it fully readable. In Table 4 we can see the last decryption of all process.

Table 4 : The last round of decryption

DECRYPTION 2								
PT	V	I	Q	I	Q	F	I	V
CT	R	E	M	E	M	B	E	R
PT	X	L	I					
CT	T	H	E					

PT	T	V	M	Z	E	X	I	
CT	P	R	I	V	A	T	E	
PT	T	E	W	W	A	S	V	H
CT	P	A	S	S	W	O	R	D

V. Conclusion

Classic cryptography is the first generation on how to make text message unreadable. However, in its algorithm, the technique is still vulnerable. By combining classical cryptography and Three-Pass Protocol, the ciphertext resulted is guaranteed. The process of sending data is no longer need to share a key to the sender of the message. Classical cryptography is considered vulnerable to attack can still be used.

References

[1]. A. P. U. Siahaan, "Factorization Hack of RSA Secret Numbers," International Journal of Engineering Trends and Technology, vol. 37, no. 1, pp. 15-18, 2016.
[2]. M. Reza dan M. A. Budiman, "Simulasi Pengamanan File Teks Menggunakan Algoritma Massey-Omura," Jurnal Dunia Teknologi Informasi, vol. 1, no. 1, pp. 20-27, 2012.
[3]. A. Dony, Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi, Yogyakarta: Andi Offset, 2008.
[4]. Mollin, An Introduction to Cryptography. Second Edition, Taylor & Francis Group, 2007.
[5]. Y. Kanamori dan S.-M. Yoo, "Quantum Three-Pass Protocol : Key Distribution Using Quantum Super Position States," International Journal of Network Security & Its Applications, vol. 1, no. 2, pp. 64-70, 2009.
[6]. B. Oktaviana, "Kombinasi Vigenere Cipher Dengan Caesar Cipher Dalam Three-Pass Protocol," Tesis. Pasca Sarjana Teknik Informatika USU, Medan, 2012.
[7]. A. P. U. Siahaan, "RC4 Technique in Visual Cryptography RGB Image Encryption," International Journal of Computer Science and Engineering, vol. 3, no. 7, pp. 1-6, 2016.
[8]. A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," International Journal of Science and Research, vol. 5, no. 3, 2016.

Authors Profile

Boni Oktaviana was born in Medan, Indonesia, in 1983. She received the S.Kom. degree in information system from Sekolah Tinggi Teknik Harapan, Medan, Indonesia in 2009, and the M.Kom. in computer science as well from the University of Sumatera Utara, Medan, Indonesia, in 2012. In 2010 he joined the Departement of Information System, Sekolah Tinggi Teknik Harapan, as a Lecturer. She plans to continue his studies this year.

Andysah Putera Utama Siahaan was born in 1980, Medan, Indonesia. He received the S.Kom. degree in computer science from Universitas Pembangunan Panca Budi, Medan, Indonesia, in 2010, and in 2012, he obtained M.Kom. from the University of Sumatera Utara, Medan, Indonesia. In 2010, he joined as a lecturer at the Department of Engineering, Universitas Pembangunan Panca Budi. He has been a researcher since 2012. He has studied his Ph. D. degree from 2016. He is now active in writing international journals and conferences.