Journal of Engineering and Applied Sciences 14 (Special Issue 9): 10669-10672, 2019
ISSN: 1816-949X

Implementation Three Pass Protocol on Multiplicative Cipher

[1]Rifaat Z. Khalaf, [2]Sarkesh K. Ridha, [3]Adel A. Abed Al-Wahab and
[4]Mohamed Khudhair Al-Gburi
[1]College of Science, University of Diyala, Diyala, Iraq
[2]College of Education For Pure Science, Karkuk University, Karkuk, Iraq
[3]College of Education For Pure Science, University of Diyala, Diyala, Iraq
[4]College of Information Technology, University of Babylon, Babil, Iraq

Abstract: A three-pass protocol one of the frameworks in cryptography that provides privacy and multiplicative cipher is one of the traditional cryptographic algorithms that based on symmetric key encryption algorithms. In this research, we used the three-pass protocol method with the multiplicative cipher by combine them, this combination allows the sender and the receiver to exchange and distribute encryption key securely, hence, they don't need to send the key because each of them using its personal key for the message encryption and decryption process, so, the security of the multiplicative cipher improved.

Key words: Cryptography, three-pass protocol, multiplicative cipher, cryptography algorithm, receiver, sender

INTRODUCTION

Nowadays, the increasing requirement for internet and its applications, impose the need to increasing the confidentiality. One of the security mechanisms that increasing the confidentiality is cryptography where it is ensure all the communications are secure (Stallings, 2008).

The basic two algorithms methods that are used are symmetric and asymmetric algorithms (Stallings, 2006). Symmetric algorithms use the same key to encrypt and decrypt data. This is generally quite fast when compared with asymmetric algorithm, the problem with this method is in order to decrypt the data the key must available and must distributed securely. For the asymmetric algorithm this method uses two keys public key and private key. The advantage of this types of algorithm is high security than symmetric algorithm but the problem with this method is slower when compared with symmetric algorithm, so it is not always suitable for every application (Bellare *et al*., 2000).

To support the security of the symmetric algorithm which is fastest, we proposed in this study new model combine one of the symmetric algorithm which is multiplicative cipher with the modern cryptography protocol which is called three-pass protocol where the first three-pass protocol was developed by Adi Shamir circa in 1980 (Rubin, 2011). And it is a framework that allows the symmetric algorithms to send encrypted message without distributed a secret key. Therefore, the advantage of this study is that we can send messages to the other parties without sharing secret key and support the multiplicative cipher in the process of sending messages.

MATERIALS AND METHODS

Multiplicative cipher: Multiplicative cipher is one of the symmetric algorithms where it uses one secret key in its application. In this algorithm, we use the encryption function: f: P → C = (a*P) MOD 26 to encrypt a message letter P to the cipher letter C. Where a is a secret key and it is relatively prime to 26, the function f produces a one-to-one relationship between the message and cipher letters which therefore, permits a one encryption. In Fig. 1, we simply test all possible keys of the multiplication ciphers MOD 26.

Now, to find the decryption function, we multiply each cipher letter by the inverse of the encryption key use the decryption function: f: C→P = (a^{-1}*P) MOD 26. Where a^{-1} is called the inverse of a, mathematically $a^{-1} * a = a * a^{-1} = 1$. We notices both (a and a^{-1}) must be correctly calculated to generate encrypt and decrypt key pair in encryption and decryption works (Beissinger and Pless, 2006).

Three-pass protocol: One of the most interesting classical cryptographic protocols is three-pass protocol (Massey, 1988). After that the protocol used in many application (Uchoa *et al*., 2007; Lim *et al*., 2008; Abdullah *et al*., 2015). The protocol declares that privacy can be obtained with no advance distribution of the secret keys or public keys. The protocol assumes that the sender and receiver connected by a classical channel that guarantees that the opponent cannot break or tamper with messages but allows the opponent to read all messages sent over the link. The sender and reciever are assumed to

Corresponding Author: Rifaat Z. Khalaf, College of Science, University of Diyala, Diyala, Iraq

PLAIN LETTER

Secret Key	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Fig. 1: Multiplicative cipher table

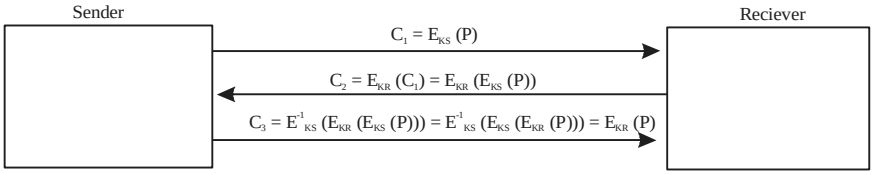

Fig. 2: Three-pass protocol

have a secret-key encryption system whose encrypting function E_k has the commutative property that is for all plaintexts P and all keys K_S and K_R:

$$E_{KS}(E_{KR}(P)) \quad (1)$$

This means that the result of a dual encryption is the same whether the sender first the key k_S the key k_R or vice versa. The step of the work of the classical three pass protocol illustrated as follows:

- The sender and receiver randomly select their own private secret keys, K_S and K_R, respectively
- The sender send a secret plaintext P to receiver, the sender encrypts P with the sender key K_S and then sends the resulting to receiver

$$C_1 = E_{KS}(P) \quad (2)$$

Then the receiver receives C_1, deals with C_1 as plaintext and encrypted C_1 with receiver key K_R. The receiver sends the resulting back to sender:

$$C_2 = E_{KR}(C_1) = E_{KR}(E_{KS}(P)) \quad (3)$$

When the sender receives C_2, decrypts C_2 with the sender key K_S. Because of the commutative property, this removes the previous encryption by K_S and the result is:

$$C_3 = E^{-1}_{KS}(E_{KR}(E_{Ks}(P))) = E^{-1}_{KS}(E_{KS}(E_{KR}(P))) = E_{KR}(P) \quad (4)$$

Then, the sender sends C_3 back to user receiver. When he receiver receives C_3, decrypts C_3 with the receiver key K_R to obtain the plaintext P that sender has successfully sent it.

In summary, the plaintext delivered in a two box securely to a receiver, the receiver using two keys to open the two box without sharing keys to open the two box, all the procedure for the classical three pass protocol shown in following Fig. 2.

Proposed algorithm: The main aim of the proposed algorithm is a secret message exchanges it between the

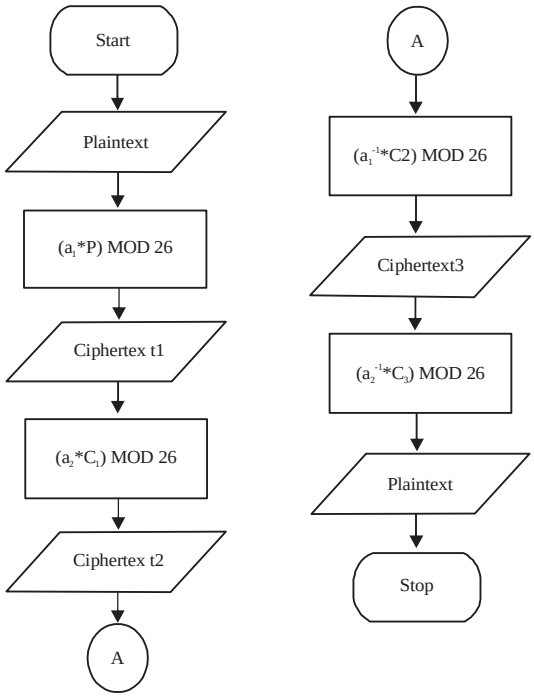

Fig. 3: Proposed algorithm work

sender and the receiver by using the multiplicative cipher and they do not need to know the secret key. In the process of encryption and decryption of the multiplicative cipher, the encryption process done twice in a row by the sender and receiver of the message using the multiplicative cipher algorithm as well as the decryption process performed twice in succession by the receiver and sender of the message. The attributes used are 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. In this combination process using a multiplicative cipher algorithm to perform encryption and decryption of messages to be sent while for the message delivery process using three pass algorithm protocol. Figure 3 is explaining the proposed algorithm work.

RESULTS AND DISCUSSION

Application of the proposed algorithm: Now, we try to prove the three-pass protocol algorithm works on multiplicative cipher. We put an incoming text "the enemy" as the plaintext. Let the key value (a_1) is 5, the sender (Alice) must encrypt the message by the formula $C_1 = (a_1 * P) \text{ MOD } 26$. Lets see illustration in Table 1.

Table 1: Encryption for Alice

T	H	E	E	N	E	M	Y
J	D	I	I	T	I	M	S

After the message has arrived at the receiver (BOB), BOB must encrypt the message by the formula $C_2 = (*C_1) \text{ MOD } 26$ (where a^{-1}_1 is the key value for Bob, let $a_2 = 9$). Let's see the illustration in Table 2.

Table 2: Encryption for Bob

1	J	C	C	X	C	M	O

After the message has arrived at the Alice, Alice must decrypt the message by the formula $C_3 = (a_{-1}1 * C_2) \text{ MOD } 26$ (where a^{-1}_1 is the inverse a_1 value for Alice, $a^{-1}_1 = 21$). Let's see the illustration in Table 3.

Table 3: Decryption for Alice

X	T	S	S	V	S	M	Q

Lastly, Bob decrypt the message P by the formula $P = (a^{-1}_1 * C_3) \text{ MOD } 26$ (where a^{-1}_1 is the inverse a_2 value for Bob,= 3). Let's see the illustration in Table 4.

Table 4: Decryption for Bob

T	H	E	E	N	E	M	Y

CONCLUSION

It is concluded that multiplicative cipher encryption can be implemented on three-pass protocol. And although, multiplicative cipher is symmetric algorithm and we know this type of cipher is less security than asymmetric because the sender and receiver should distribute the secret key but because of three-pass protocol help the algorithm to distribution the key and increase the confidentiality of the algorithm, hence, the proposed algorithm became more secure.

In this research, we simply apply protects messages using the standard alphabet consists of 26 characters for future research, may be applied to a more complex character.

REFERENCES

Abdullah, A.A., R. Khalaf and M. Riza, 2015. A realizable quantum three-pass protocol authentication based on hill-cipher algorithm. Math. Prob. Eng., 2015: 1-6.

Beissinger, J. and V. Pless, 2006. The Cryptoclub: Using Mathematics to Make and Break Secret Codes. CRC Press, Boca Raton, Florida, USA., ISBN:9781568812236, Pages: 200.

Bellare, M., A. Boldyreva and S. Micali, 2000. Public-key encryption in a multi-user setting: Security proofs and improvements. Proceedings of the International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT 2000), May 14-18, 2000, Springer, Berlin, Germany, ISBN:978-3-540-67517-4, pp: 259-274.

Lim, M.H., C.M. Yeoh, S. Lee, H. Lim and H. Lee, 2008. A secure and efficient three-pass authenticated key agreement protocol based on elliptic curves. Proceedings of the International Conference on Research in Networking, May 5-9, 2008, Springer, Singapore, ISBN:978-3-540-79548-3, pp: 170-182.

Massey, J.L., 1988. An introduction to contemporary cryptology. Proc. IEEE., 76: 533-549.

Rubin, F., 2011. Device, system and method for fast secure message encryption without key distribution. U.S. Patent and Trademark Office, Washington, DC. USA. https://patents.google. com/patent/ US7907723B2/en.

Stallings, W., 2006. Cryptography and Network Security: Principles and Practices. 4th Edn., Prentice-Hall, Upper Saddle River, New Jersey, USA., ISBN-10: 013 1873164, pp: 97-119.

Stallings, W., 2008. Computer Security: Principles and Practice. Pearson Education India, India, ISBN:9788131733516, Pages: 799?.

Uchoa, A.G.D., M.E. Pellenz, A.O. Santin and C.A. Maziero, 2007. A three-pass protocol for cryptography based on padding for wireless networks. Proceeding of the 2007 4th IEEE International Conference on Consumer Communications and Networking, January 11-13, 2007, IEEE, Las Vegas, Nevada, USA., pp: 287-291.