International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 16 (2019) pp. 3531-3536
© Research India Publications. http://www.ripublication.com

Improvement of Classical Cipher Algorithm based on a New Model of Timed-Released Encryption

Wisam. Ch. Alisawi*[+], Zahraa Ch. Oleiwi*, Wasan A. Alawsi*, Ali S. Alfoudi and Nagham K. Hadi****

**Faculty of Science, University of Al-Qadisiyah*
***College of Computer Science and Information Technology, University of Al-Qadisiyah*

[+]*Correspondence author*

Abstract

A new technique of time-released encryption was proposed to improve the security of classical cipher algorithm. Classical cipher method has less computation complexity than other encryption methods but, it is considered to be weak against hacker attack. Therefore, the improvement of this method via using time-locked encryption can decipher after passing a specific time-,and will overcome the drawback of being weak security. The proposed new approach of highly secure timed-locked encryption based classical cipher methods have numbers of desirable properties including but not limited to, self-identified time-based key updates, less complexity and key protection. Analysis results show that the proposed algorithm satisfies all security requirements (confident, integrity and authentication).

Keywords: classical cipher methods; release time; time-based key; highly secure

1. INTRODUCTION

The term timed-released encryption (TRE) represents the idea of encrypting the message so that it cannot be read (or decrypted) by anyone, including the designated recipients of the message, until predetermined “release time”, selected by the sender. [1].

The traditional cipher method (TCM) is divided into two types, transposition (rearrange letter) and Substitution (replace letter). The TCM is unusable due its weakness, but it is considered to be the backbone for with less time process [2].

Generally, the requirement of security system represent the general aims of research. One of these requirements is the strong encryption algorithm against potential attacks. Tradeoff between time of process and computation complexity is considered one of the security challenges[3, 4].

In this article, a new technique model proposed to achieve strong method with less complexity by using classical cipher method with time –released system to overcome weakness of these classical method as well as make benefit from time –released encryption. In the proposed method a specific algorithm based on time key has been modified, such that not adversary can know any information or data in the message even when the deadline is passed. Where the deadline update automatically will vary with every attempt to read the message from adversary. Analysis study of new proposed security model in term of confident, integrity, authentication and computation complexity is present in order to satisfy the goals and requirements of high performance security system.

This article was organized as follows. First, the related work is presented in Section 2. Section 3 describes the time-**released encryption**. Section 4 describes the algorithms and example of a **new proposed time-released algorithm**. Section 5 explains the analysis results according to security and complexity of the proposed model. Finally, the conclusions is presented in Section 6.

2. RELATED WORK

Cryptographic mechanisms are important security component of any operating system to secure the system itself and its communication paths. Indeed, in many situations, cryptography is considered to be the only tool that can solve a particular problem. It is the practice and study of techniques for secure communication in the presence of third parties. Modern cryptography is highly based on mathematical theory, computer science practice, and cryptographic algorithms [5].

TRE problem was posed in the 1990s, and several modifications were proposed for TRE programs based on the two approaches, TSA [6-16] and TLP [1, 17-21]. However, none of them is optimum.

Existing TSA-based methods require several interactions, including server with sender [1] and server with receiver [22], and the server should be allowed to know and pass all the secret keys [23] and/or messages [6].

Security model for non-interactive timed-release encryption schemes was suggested previously with a new efficient construction fitting. [24].

In [26] a new construction of a witness encryption scheme, which is of independent interest, was proposed. This scheme, based on Subset- Sum, achieves extractable security without relying on obfuscation.

All of the above has generated the idea of our research based on building a simple and powerful model that can work with traditional algorithms to gain more strength and security. This will be explained in detail in the following paragraphs

3. TIME –RELEASED ENCRYPTION

A timed-release cryptosystem proposed by R.L. Rivest, et al. [1] was called the "time-lock puzzle" (TLP). This approach has been developed for protecting information, and it is related precisely to the problems that arise when sending a secret message to the future. Its specificity depends on the fact that unlike traditional cryptographic methods that assume that the recipient of a secret message has the sender's secret key (in symmetric cryptosystems) or the sender of a message has the recipient's authentic public key (in asymmetric cryptosystems), the secret key is destroyed immediately after encryption and it is unknown to both the sender and the recipient of the message.

At present, there are two main methods for constructing timed-release cryptosystems[6]:

- Time-lock puzzle (TLP) which is depends on the basis of computational problems with sequential algorithms for solving
- The use of trusted servers (or agents), undertaking the obligation not to disclose information for a specified period of time.

In general, the cryptographic task of message encryption was considered so that the received cryptogram can be decrypted (including by the sender of the message) after a specified time interval. An attack on such a cryptosystem is considered successful if it is possible to decrypt the message much earlier than specified time. This method of protection, with the ability to disclose sensitive information after a certain time, is called timed-release crypto [11, 12].

4. PROPOSED TECHNIQUE

Figures (1) and (2) show the scheme of the proposed security model. Where the general components of the proposed new time released technique were illustrated in these figures. Figure (1) shows the work of the modified TRE method against the passive opponent (capture the copy of decrypted message).

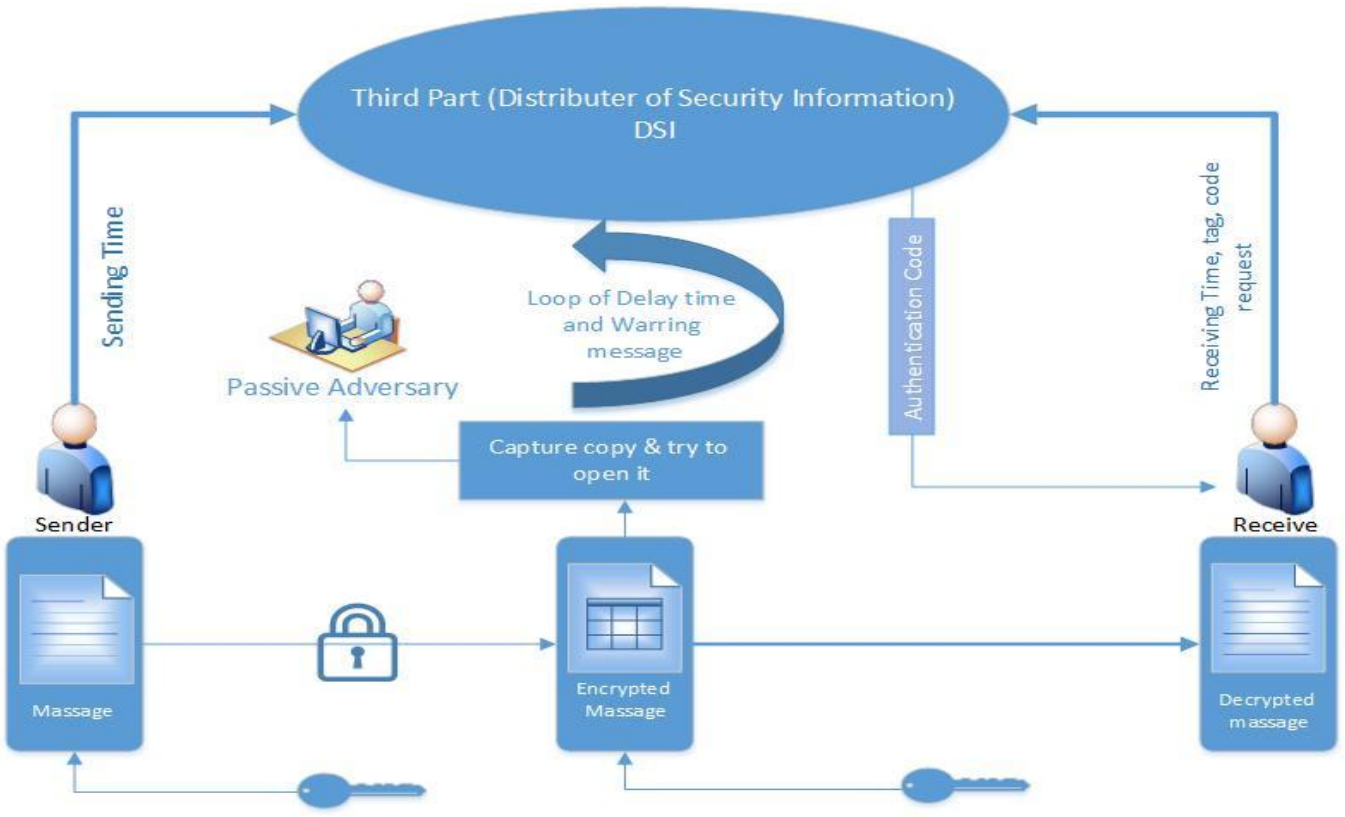
Third Part (Distributer of Security Information)
DSI
Sending Time
Loop of Delay time and Warring message
Passive Adversary
Authentication Code
Receiving Time, tag, code request
Capture copy & try to open it
Sender
Receive
Massage
Encrypted Massage
Decrypted massage

Figure 1: Proposed model of time release encryption with respect to passive adversary

While, Figure (2) shows the work of the proposed method against active opponent (read the message, change it, and retransmit it).

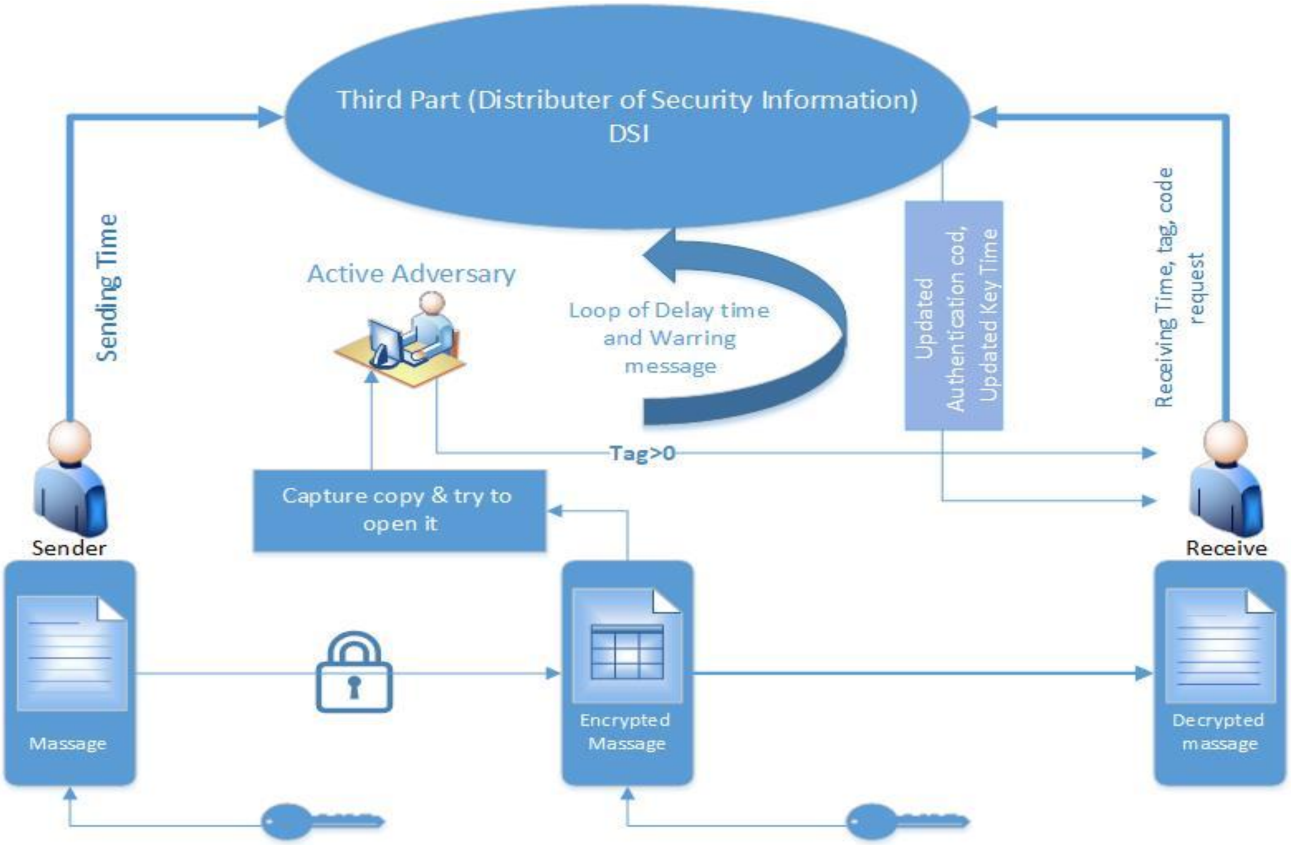
Third Part (Distributer of Security Information)
DSI
Sending Time
Active Adversary
Loop of Delay time and Warring message
Updated Authentication cod, Updated Key Time
Receiving Time, tag, code request
Tag>0
Sender
Receive
Capture copy & try to open it
Massage
Encrypted Massage
Decrypted massage

Figure 2: Proposed model of time release encryption with respect to active adversary

4.1 New proposed time-released algorithm

As shown in algorithms (1) and (2) the sender locks the cipher message with specific time so that any one try to read the message before dead time will enter in loop of delay time depending on increase tag counter. In addition, warning message, send to security information distributer as adverse detection.

Second case was treated in algorithm (1) when the receiver receives the message after it is resend by the adverse, so the received time be more than release time; in this case decipher depend on authcode request from security information distributer.

Algorithm 1 Lock message with keytime

```
//Notation Description:
// tag: represent number of trials to open message
//authcode: represent authentication code
//authcode no: arbitrary umber used for update time delay automatically
{
Read authcode
Tag=0      % no trial
If ( instant time< received time) or (instant time>= received time & tag>0 & authcode false ){
Tag=tag+1;    %update tag
Update authcode no.
Call delay time function
Delay time=delay time+ authcode no.
Send warning message to security information distributer
}
Else If (instant time>= received time & tag=0) or (instant time>= received time & tag>0 & authcode true){
Delay time=keytime
Allow read message and decrypt
}
}
```

Algorithm 2 encryption algorithm at sender side

```
//Notation Description:
// M: original message
//C: encryption message
// $K_E$: arbitrary: encryption key
{
Call encryption algorithm function
C=(M,$K_E$)
Set  tag=0    authcod no.=0
Call Lock message with keytime algorithm
Send (C, tag) to receiver
Send (TIME OF SEND) to security information distributer
}
```

Algorithm 3 decryption algorithm at receiver side

```
//Notation Description:
// M: original message
//C: encryption message
// $K_E$: arbitrary: encryption key
{
Send request to center (tag, time of receive)
Call decryption algorithm
M=(C,$K_E$)
}
```

Algorithm 4 Security Information Distributer Request

```
If tag =0 then {
send original  key time and authcode to receiver
}
Else
Send update time key and  update authcode
```

4.2 Experimental Example

Proposed algorithm was implemented using MATLAB, and it can be clarified as below example:

At time of sending message is 2:00 am and released time 10 seconds then:

First case: when the massage reach to receiver without adverse interaction the received time equal or more than 2:10 with tag=0 then the message can be decrypted successively.

Second case: When there is try to read the message before 2:10 by ***active adverse*** then:

1- Tag is increased.

2- Alarm message is sent to security information distributer.

3- Delay time function is active.

4- Authcode no. is update with each trial.

Third case: the receivers receive the message after 2:10 and tag >0 then

1- The receiver send the authcode request to security information distributer

2- The receiver uses authcode to decipher the message after dead time.

Fourth case: When there is try to read the message before 2:10 by **passive adverse** then:

1- the receiver receive the message at or after 2:10 and tag =0,then he will decrypt the message successively

2- Passive adverse cannot open the message because he or she does not have authcode after dead time. On the other hand, if they try to open the message before 2:10 he or she will inter time delay loop.

5. ANALYSIS RESULT

The proposed encryption methods analysis was performed in terms of security requirement and performance of algorithm complexity such as:

5.1 Security Analysis

1- Confidentiality

It means protection against unauthorized access to information of message[2], so that the proposed scheme of encryption method satisfies this property since it includes cipher method with cipher and time keys.

2- Integrity

It is the protection against active attacks, i.e. avoid information in message from modification [2]. Integrity was satisfied by notice that any attempt to open the message during the period of deadline can be detected by automatic alarm sent to receiver email as in Algorithm of time- release encryption and loop of time delay technique,

3- Authentication

This is the assurance of receiver identity [2]. Since the authentication code is used, proposed method meets authentication security requirement.

4- Signature

To avoid denial, the receiver can decrypt the cipher message only after deadline depending on the number of the passing tries and push the active and passive attack in the loop of time delay, as such it has a mean of signature [2].

5.2 Performance And Complexity Analysis

The complex theory is a branch of the theory of computing in computer science theory and mathematics, and this theory was concentrated on the classification of computer problems by their difficulty as well as in linking the sections of complexity (complexity classes) [26].

The computational complexity theory allows different cryptographic techniques and algorithms to be compared and determines how safe and secret they are. The complexity of the algorithm is determined using the computing capabilities required to implement. The computational complexity is measured by two variables [27]:

1- Time restriction

2. Complexity of space

To obtain an evaluation of the proposed method, we calculated the time complexity of the new method compared to the original method. The time of computation complexity of the proposed method will not affect the overall calculation of the accompanying method if the message is not exposed to hacker. If the message is truncated, the complexity time will be O(n). From this, we see that the sum of the complexity of the added method will not affect any algorithm accompanying it.

6. CONCLUSION

A new approach that can improve the performance of the traditional cipher method and make benefit of its simplicity by using time released technique is proposed. The proposed algorithm to implement this approach is present and analysis study of its performance in term of security requirement is discussed. Analysis result proved that the complexity of the new method does not exceed the complexity of the classical method. Meanwhile, the complexity of cryptanalysis increased with O(n) thereby this method improved and became robust against attack. On the other hand, this new approach based on time-released satisfies integrity and authorization since it cannot be processed before a specific deadline (key of time).

Acknowledgement

The Authors would like to thank the Ministry of Higher Education & Scientific Research (Iraq) and the Faculty of Science, University of Al-Qadisiyah for the financial support of this project

REFERENCES

[1] Rivest, R.L. et al., Time-lock puzzles and timed-release crypto, Massachusetts Institute of Technology, (1996).

[2] W. Stallings, Cryptography and Network Security Principles And Practice, Prentice Hall, (2006).

[3] Salah, A.K. Albermany et.al., S-RADG: A Stream Cipher RADG Cryptography, International Journal of Scientific & Engineering Research Volume 9, Issue 3, March(2018).

[4] Chalkias , K., et al., An Implementation Infrastructure for Server-Passive Timed-Release Cryptography, 2008 The Fourth International Conference on Information Assurance and Security, IEEE, (2008).

[5] Zaru, Z. A., General Summary of Cryptography, Journal of Engineering Research and Application, (2018).

[6] Cheon, J. H., et al., Timed-Release and Key-Insulated Public Key Encryption, International Conference on Financial Cryptography and Data Security, Springer, (2006)

[7] Boneh, D., Franklin, M., Identity-based encryption from the weil pairing, Springer, (2001).

[8] Hwang, Y.H. et al., Timed-Release Encryption with Pre-open Capability and Its Application, Springer, (2005).

[9] Cathalo, J. et al., Efficient and Non-Interactive Timed-Release Encryption, Springer, (2005).

[10] Cheon, J.H. et al., Provably Secure Timed-Release Public Key Encryption, ACM Transactions on Information and Systems Security, (2008).

[11] Chow, S.S.M. et al., General Certificateless Encryption and Timed-Release Encryption, Springer, (2008).

[12] Chow, S.S.M., Yiu, S.M., Timed-Release Encryption Revisited, Springer, (2008).

[13] Dent, A.W., Tang, Q., Revisiting the Security Model for Timed-Release Encryption with Pre-open Capability, Springer, (2007)

[14] Fujioka, A. et al., Generic Construction of Strongly Secure Timed-Release Public-Key Encryption, Springer, (2011).

[15] Matsuda, T. et al., Efficient Generic Constructions of Timed-Release Encryption with Pre-open Capability, Springer, (2010).

[16] Nakai, Y. et al., A Generic Construction of Timed-Release Encryption with Pre-open Capability, Springer, (2009).

[17] Paterson, K.G., Quaglia E.A., Time-Specific Encryption, Springer (2010).

[18] Mao, W., Timed-release cryptography, Springer, (2001).

[19] Boneh, D., Naor, M., Timed commitments, Springer, (2000).

[20] Garay, J., Jakobsson, M., Timed release of standard digital signatures, Springer, (2002).

[21] Garay, J., Pomerance, C., Timed fair exchange of standard signatures, Springer, (2003).

[22] Di Crescenzo, G. et al., Conditional oblivious transfer and time-release encryption, Springer, (1999).

[23] Boneh, D., Franklin, M., Identity-based encryption from the weil pairing, Springer, (2001).

[24] Cathalo, J., Libert, B., and Quisquater, J., Efficient and Non-interactive Timed-Release, Springer, (2005).

[25] Liu, J., Jager, T., and Kakvi, S. A., How to build time-lock encryption, Springer, (2018).

[26] N. D. Jones, Computability and Complexity From a Programming Perspective, The MIT Press Cambridge, Massachusetts London, England, (1997).

[27] H. zherah, Studying of Secret Sharing Schemes and, Research For Master degree, Syrian Arab Republic, (2009).