Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm

Dian Rachmawati 1*, Amer Sharif 1*, Jaysilen 1*, and Mohammad Andri Budiman 1*

1Program Studi S1 Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Jl. Alumni No 9-A, Medan 20155, Indonesia

*Email: dian.rachmawati@usu.ac.id, amersharifdjamin@gmail.com, jaysilen07@gmail.com, mandrib@usu.ac.id

Abstract. Security becomes a very important issue in data transmission and there are so many methods to make files more secure. One of that method is cryptography. Cryptography is a method to secure file by writing the hidden code to cover the original file. Therefore, if the people do not involve in cryptography, they cannot decrypt the hidden code to read the original file. There are many methods are used in cryptography, one of that method is hybrid cryptosystem. A hybrid cryptosystem is a method that uses a symmetric algorithm to secure the file and use an asymmetric algorithm to secure the symmetric algorithm key. In this research, TEA algorithm is used as symmetric algorithm and LUC algorithm is used as an asymmetric algorithm. The system is tested by encrypting and decrypting the file by using TEA algorithm and using LUC algorithm to encrypt and decrypt the TEA key. The result of this research is by using TEA Algorithm to encrypt the file, the cipher text form is the character from ASCII (American Standard for Information Interchange) table in the form of hexadecimal numbers and the cipher text size increase by sixteen bytes as the plaintext length is increased by eight characters.

1. Introduction

Cryptography is a method to send the file in secret, which is mean only the recipient can read the file [1]. Cryptography has its etymology, kryptos means hidden, and graphein means to write [2]. Based on its etymology, cryptography is a technique to secure file by encoding the original file to become some scramble code which is difficult to understand by the public [2]. There is two main process in cryptography, the process of transform file into scramble code is called encryption and the process to reverse the scramble code back to the original file is called decryption [3].

In this research, three main components in cryptography are used, which is cipher text, plaintext, and the keys. Cipher text is the scramble code to secure the original file [2] and plaintext is a file that needs to be secured [2].

Tiny Encryption Algorithm (TEA) is a symmetric algorithm which is found by David Wheeler and Roger Needham from Cambridge University. TEA is designed to be fastest and most efficient cryptographic algorithm compared to other symmetric algorithms like IDEA, DES, and AES [4]. The
plaintext is divided into two halves and the key is divided into four 32-bit blocks [5]. XOR, ADD, and SHIFT operator are used in encryption and decryption process, which means the cipher text size is small and easy to send to recipient [6]. The same key is used by TEA for encryption and decryption process, it mean that the security of this algorithm depends on its key. Once the key is divulged, everyone can encrypt and decrypt the file.[2]

LUC is an asymmetric algorithm developed by Peter Smith and Michael Lennon based on Lucas Function. LUC algorithm has two different keys which mean the security of this algorithm does not depend on its key. LUC public keys are used to encrypt plaintext and LUC private key is used to decrypt the cipher text [7].

LUC Algorithm has key generation phase in order to produce LUC public key to encrypt plaintext and LUC private key to decrypt the cipher text. Even the LUC public key can be made public [2]. Although LUC public key is so secure, it produces huge size cipher text and sender will be difficult to send the cipher text to the recipient.

Hybrid Cryptosystem is a method to secure file by combining both of symmetric and asymmetric algorithm in order to secure plaintext [3]. In the hybrid cryptosystem, a file is secured by using the symmetric algorithm and symmetric key is secured by using asymmetric algorithm [3]. By using this method, the sender has small-size cipher text because plaintext is secured by the symmetric algorithm and secure key because a symmetric key is secured by asymmetric algorithm. In this research, TEA is used as symmetric algorithm and LUC algorithm is used as asymmetric algorithm.

2. Method
The scheme of securing file by using a hybrid cryptosystem method is showed on Figure 1.

![Figure 1 Hybrid Cryptosystem Method Scheme](image-url)
Based on figure 1, the first step to using hybrid cryptosystem method is generate LUC public key and the LUC private key by following this step [8].

- Select two large prime number (P, Q) and P must be co-prime to Q or GCD (Greatest Common Division) between P and Q is 1
- Calculate the value of N by using this equation:
  \[ N = P \times Q \] (1)
- Calculate the euler function (T) by using this equation:
  \[ T = (P - 1) \times (P + 1) \times (Q - 1) \times (Q + 1) \] (2)
- Select the random number (E) and E is smaller than T but larger than 1
- check if E is co-prime to T or not.
- If E is co-prime to T, then E is the LUC public key
- Calculate the R(N) value by using this equation:
  \[ R(N) = LCM \{ (P - 1) \times (P + 1) \times (Q - 1) \times (Q + 1) \} \] (3)
- Calculate the D value iteratively until D reach this equation:
  \[ D \times E \mod R(N) = 1 \] (4)
- After D value is generated, then D is the LUC private key.

After both of keys are generated, recipient send LUC public key to sender, so sender can use the LUC public key to encrypt the TEA key. Before encrypt the TEA key, sender must encrypt the file first using TEA key in order to produce ciphertext by following this step: [6]

- Convert plaintext and key into encoding table. In this research, the ASCII (American Standard for Information Interchange) encoding table is used,
- Divide the plaintext into two blocks and each block have 32-bit data (block Y [0], Block Z [0])
- split the key into four blocks and each block have 32-bit data (block K [0], block K [1], block K [2], block K [3])
- Using this Equation to start encryption:
  \[ Y[i+1] = Y[i] + ((Z[i] <<4) + K[0]) \times (Z[i] + \text{delta}) \times ((Z[i] >> 5) + K[1])) \] (5)
  \[ Z[i+1] = Z[i] + ((Y[i] <<4) + K[2]) \times (Y[i] + \text{delta}) \times ((Y[i] >> 5) + K[3])) \] (6)
  \[ 0 \leq i \leq 31; \text{ i is Natural Number; } \]
  Delta is the golden number or 9E3779B9
  The cipher text will be available in block Y [32] and in block Z [32].

Sender encrypt the TEA key by using LUC public key which is already accepted from recipient earlier by following this step [7]:

- Convert The TEA key into encoding table
- Input LUC Encryption Key (e)
- Using this pattern:
  \[ V[0] = 2 \] (7)
  \[ V[1] = \text{TEA Key} \times P \] (8)
  \[ V[i] = (P \times V[i-1] - V[i-2]) \mod N; i \geq 2 \] (9)
- Repeat the (8) process until I = E
  \[ V[E] = (P \times V[e-1] - V[e-2]) \mod N. \] (10)
- V[E] is the cipher key or \(V[E] = C\).

After recipient accept both of cipher text and cipher key, recipient uses LUC Private Key to decrypt the cipher key in order to produce the TEA key by following this step [8]:

- Select the cipher key
- Input LUC Decryption Key (d)
- Using this pattern:
  \[ V[0] = 2 \] (11)
  \[ V[1] = \text{Cipherkey} \times C \] (12)
  \[ V[i] = (C \times V[i-1] - V[i-2]) \mod N i \geq 2. \] (13)
When \( I = d \), use this equation :

\[
 V[d] = (C \times V[d - 1] - V[d - 2]) \mod N.
\]  

(14)

\( V[d] \) is the TEA Key

After TEA key is produced, recipient can use it to decrypt the ciphertext by following this step [4] :

- Divide the cipher text into two halves, and each halve have 32-bit data (block \( Y[32] \), Block \( Z[32] \))
- Divide the key into four blocks, and each block have 32-bit data (block \( K[0] \), block \( K[1] \), block \( K[2] \), block \( K[3] \))
- Using this Equation to start Encryption.

\[
 Y[i-1] = Y[i] - ((Z[i] << 4) + K[0]) \land (Z[i] + \text{delta}) \land ((Z[i] >> 5) + K[1]))
\]  

(15)

\[
 Z[i-1] = Z[i] - ((Y[i] << 4) + K[2]) \land (Y[i] + \text{delta}) \land ((Y[i] >> 5) + K[3]))
\]  

(16)

\( i \) start from 32 down to 1; \( i \) is a Natural Number

\( \text{Delta} \) is the golden number or 9E3779B9

- Plaintext will come out when it reach block \( Y[0] \) and block \( Z[0] \)

After recipient decrypts the ciphertext, the hybrid cryptosystem method to secure file already done. Because sender use a symmetric algorithm (TEA) to encrypt the file and an asymmetric algorithm (LUC Public Key) to encrypt the TEA Key. Meanwhile, recipients use the asymmetric algorithm (LUC Private Key) to decrypt the cipher key in order to produce the TEA key which is used to decrypt the ciphertext.

3. Results and Discussions

These experiments are conducted on the Windows 10 Pro Creator Update Notebook which has 64-bit architecture Intel Core i3 processor and 4096 MB RAM. The result of this research is presented in Table 1 as follows:

| Table 1. The Comparison between plaintext size and ciphertext size |
|---------------------------------------------------------------|
| Sample Number | Plaintext size (byte) | Ciphertext size (byte) |
|----------------|------------------------|------------------------|
| 1              | 1                      | 16                     |
| 2              | 2                      | 16                     |
| 3              | 8                      | 16                     |
| 4              | 9                      | 32                     |
| 5              | 10                     | 32                     |
| 6              | 17                     | 48                     |
| 7              | 18                     | 48                     |
| 8              | 25                     | 64                     |
| 9              | 33                     | 80                     |
| 10             | 41                     | 96                     |
| 11             | 56                     | 112                    |
| 12             | 95                     | 192                    |
| 13             | 96                     | 208                    |
| 14             | 106                    | 224                    |
| 15             | 112                    | 224                    |

Table 1 shows when the plaintext size is increased by eight characters, the ciphertext size will increase by sixteen bytes.
The integrity is the main purpose in cryptography, that means the file was sent by the sender, the same file must be accepted by a recipient and there is the result of securing file by using hybrid cryptosystem method as shown in Figure 2.

Figure 2: File Encrypted into Ciphertext

Based on figure 2, the plaintext has been encrypted by using TEA key and produce ciphertext. Because hybrid cryptosystem method is used to secure file, the sender must encrypt the TEA key use LUC Public Key, which is available on Figure 3.

Figure 3: The TEA Key is encrypted by using LUC Public Key

After the TEA key is encrypted and produce the cipher key, both of cipher key and ciphertext is sent to a recipient. Then, recipient use LUC private key to decrypt the cipher key on Figure 4.
The recipient already have the TEA key to decrypt the ciphertext which is showed on Figure 5.

Figure 4 and Figure 5 show hybrid cryptosystem method has met the requirement of the integrity aspect on cryptography because recipient accepts the same file and the same key which was sent by the user before.

4. Conclusions
The conclusion of this research is TEA key is used to encrypt the plaintext and decrypt the ciphertext, meanwhile, LUC Algorithm is used to encrypt the TEA key and decrypt the cipher key. The hybrid cryptosystem method by using TEA and LUC Algorithm met the requirement of the integrity aspect on cryptography. The ciphertext size is increased by sixteen bytes as the plaintext length is increased by eight characters. This system can secure the file which has this extension: *.pdf, *.txt, *.rtf, *.doc, *.docx, and *.otd.

Acknowledgments
The authors gratefully acknowledge that the present research is supported by Fund Dissemination IPTEKS Research Results for Lecturers / Researchers Universitas Sumatera Utara.

References
[1] R. Mollin, An Introduction to Cryptography, 2nd Ed., Florida: Chapman & Hall/CRC, 2007.
[2] B. Schneier, Applied Cryptography, 2nd Ed., John Wiley & Sons, Inc, 1996.

[3] N. Smart, Cryptography: An Introduction, 3rd Ed., Bristol City, 1999.

[4] S. A. Y. Hunn, S. Z. Naziri and N. Idris, “The Development of Tiny Encryption Algorithm (TEA) Crypto-Core for Mobile Systems,” IEEE International Conference on Electronics Design, Systems and Applications, pp. 45-49, 2012.

[5] J. Balakrishna, P. Daniel, and R. Chandel “Design & Implementation of VLSI Architecture for XTEA,” International Conference on Advanced Computing, Communication and Network, Hamirpur, 2011.

[6] D. Wheeler, R. Needham “TEA, a Tiny Encryption Algorithm”, First International Conference on Security in Pervasive Computing, Boppard, 2003.

[7] Z. M. Ali, “Parallel Computation Algorithm for LUC Cryptosystem Based on Binary Number,” Journal of Theoretical And Applied Information Technology, vol. 44, no. 1, pp. 12-21, 2012.

[8] P. J. Smith and M. J. J. Lennon, LUC: A New Public Key System, Auckland: The University of Auckland, 1993.