Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023
DOI : https://doi.org/10.33395/sinkron.v8i2.12202
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Performance Analysis Of The Combination Of Advanced Encryption Standard Cryptography Algorithms With Luc For Text Security

Wahyu Ady Putra[1)*], Suyanto[2)], Muhammad Zarlis[3)],
[1)]Master of Informatics Program, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara,
[2)]Department of Mathematics, Faculty of Mathematics and Natural Science, Universitas Sumatera Utara,
[3)]Information Systems Management Department, BINUS Graduate Program – Master of Information Systems Management, Bina Nusantara University, Jakarta, 11480, Indonesia
[1)]wahdyp@gmail.com, [2)]suyanto@usu.ac.id, [3)]muhammad.zarlis@binus.edu

Submitted : Feb 14, 2023 | **Accepted** : Apr 3, 2023 | **Published** : Apr 5, 2023

Abstract: Data security is very important as it is easy to exchange data today. Cryptographic techniques are needed as data security techniques. Combining two cryptographic algorithms is a solution for a better level of security. The Advanced Encryption Standard (AES) cryptographic algorithm requires low computational power and is the best symmetric algorithm. The LUC algorithm is an asymmetric algorithm that was developed from the RSA algorithm and has advantages in a better level of security and processing speed. In this research, two symmetric and asymmetric cryptographic algorithms will be combined in a hybrid scheme, namely the AES and LUC algorithms to improve data security. the AES algorithm will encrypt and decrypt messages, while the LUC algorithm performs encryption and decryption of the AES key. The results showed that the combination of the two AES and LUC algorithms was successful. However, the computational time needed by the two algorithms to perform the encryption and decryption process increases. The simulation results of the brute force attack performed show that the LUC algorithm can still be attacked. The greater the value of E (the public key of the LUC algorithm), the longer it takes for the brute force attack to be successful. The value of E is also directly proportional to the computational time required by the LUC. So it can be concluded that the AES algorithm is less precise when combined with the LUC algorithm.

Keywords: AES; LUC; Text Security; hybrid cryptographic; cryptographic

INTRODUCTION

Exchange of information and data becomes very practical, fast and easy in line with the rapid development of information technology today. The data sent must be kept secure because it contains very important and even confidential information. To prevent data or information theft, cryptography is needed as a technique for encoding data or information [1]

With cryptographic techniques, it can be ensured that the data and information sent are protected from various threats from unauthorized parties. Two types of cryptographic algorithms that are commonly used are symmetric and asymmetric cryptographic algorithms. The symmetric algorithm has a quick processing time because this algorithm performs the encryption and decryption process using the same 1 key and is small in size, but is insecure when exchanging keys. Unlike the asymmetric

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i2.12202 p-ISSN : 2541-044X

algorithm which uses 2 different keys and a large key size so that the processing time is long [2]. Combining two cryptographic algorithms is a solution for a better level of security and faster processing time[3].

The Advanced Encryption Standard (AES) cryptographic algorithm is one of the best symmetric cryptographic algorithms and requires low computational power. In the AES algorithm, the plaintext bits are divided into blocks of bits of the same length, which are known as cipher blocks. The use of 128-bit blocks in the AES algorithm has advantages in terms of efficiency and better security than other symmetric algorithms such as DES and 3DES [4]. Brute force attacks are one of the weaknesses of the AES algorithm, even though cryptanalysts need hard work to do it [5].

The LUC algorithm is an asymmetric algorithm developed from the RSA algorithm. This algorithm has the advantage of a better level of security and processing speed [6]. Just like other asymmetric cryptographic algorithms, the LUC algorithm has the disadvantage of long computation time and the need for large storage.

A combination of algorithms will be carried out using the AES algorithm to encrypt and decrypt messages, and the LUC algorithm to encrypt and decrypt the AES external key. By combining the two AES algorithms with the LUC algorithm, it is hoped that there will be an increase in the security of the resulting algorithm.

LITERATURE REVIEW

lavich [3] in his research on the combined implementation of the aes and elgamal algorithms for flight control systems explained that the application of the algorithm to the system carried out still needs to be improved or developed with other cryptographic algorithms to improve the description process faster and lower memory consumption.

Sari [6] in his research on a comparison between the LUC, ElGama and RSA algorithms explained that based on the tests that have been carried out the LUC algorithm has the fastest encryption processing time among the three algorithms.

METHOD

This study aims to analyze and see the performance of a combination of symmetric algorithms using AES cryptography and LUC asymmetry algorithms in a hybrid scheme. The process of plaintext encryption and ciphertext decryption is carried out using the AES algorithm, then the AES key will be encrypted and decrypted using the LUC algorithm. This study uses python programming language to assist this research.

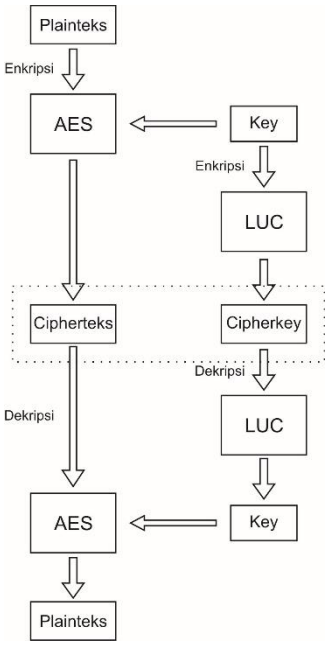

Figure 1. Research design

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i2.12202 p-ISSN : 2541-044X

In the research design conducted in Figure 1 it can be explained as follows:
Encryption process:
1. Plaintext is encrypted using the AES-128 algorithm to produce ciphertext.
2. The AES-128 algorithm key is encrypted using the LUC algorithm to produce a cipherkey.
Decryption process:
3. The cipherkey is decrypted using the LUC algorithm and generates a key.
4. The ciphertext is decrypted using the AES-128 algorithm and produces plaintext.

In this study, a simulation of a brute force attack will also be carried out against the LUC algorithm, which in combining the algorithms acts as a security against the AES algorithm key.

AES Algorithm

The next figure 2 illustrates the encryption /decryption rounds of the AES-128. The cipher maintains an internal 4×4 matrix of bytes referred to State, on which the operations are performed. Initially, State is filled with the input data block and exclusive-ORed with the encryption key.

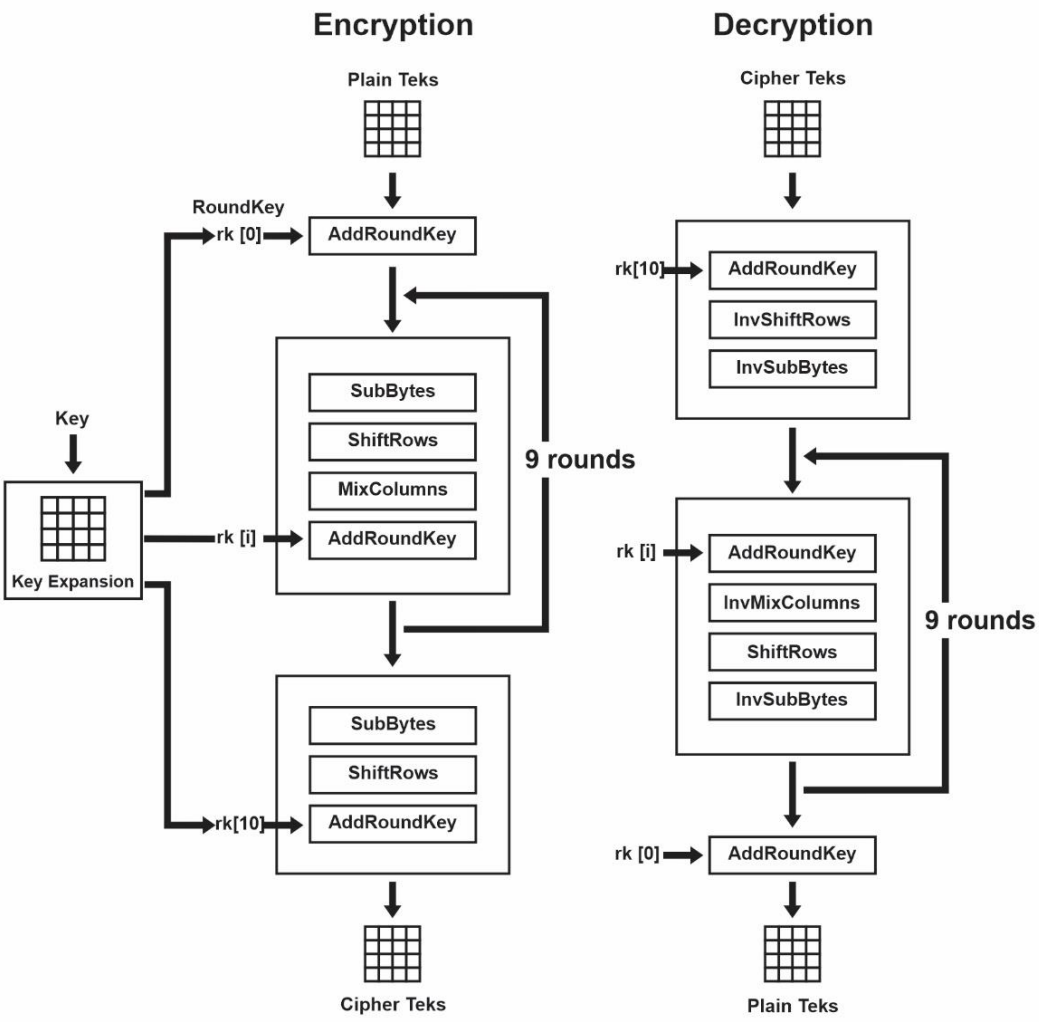

Figure 2. AES encryption/decryption

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i2.12202 p-ISSN : 2541-044X

The Operations involved by AES are :

- Key Expansion : this operation generates RoundKey for the Rounds to encrypt/decrypt messages.
- Initial Round (Round 0) : realize the AddRoundKey where the input data block of 128 bits is XORed with the initial 128 bits key which will generate the nine round keys.
- Nine identical Rounds (Round 1-9): from the first round to the ninth round, the following four transformations are executed sequentially :

  1. SubBytes –a linear substitution where each byte is replaced by another one found in a specific substitution table related to AES, the S-Box.
  2. ShiftRows –a transposition where each row of the state matrix is cyclically shifted by 0, 1, 2 or 3 bytes respectively.
  3. MixColumns –this transformation operates on the state column by column, treating each column as four-term polynomial. The columns are considered in the Galois field GF (2^8) and multiplied by a fixed polynomial a(x) modulo x4+1 given by: a(x) = (03) x3 + (01) x2 + (02)
  4. AddRoundKey calculates a XOR between the state matrix at the input and a Roundkey. It is the sole operation that involves the Roundkey value.

- Final Round (Round 10): bypasses the MixColumns transformation.

The AES decryption operation is the inverse of the encryption operation where the four transformations are performed in the reverse order.

LUC Algorithm

LUC algorithm is built based on mathematical functions, that is Lucas Sequence [6] :

$$fluc\ (P) = Vn\ (P, 1)\ mod\ N \qquad (1)$$

The three main process in the LUC algorithm are the key generator, encryption process, the decryption process. The process stages of the key generator will be explained as follows :

1. Multiply two prime numbers p and q and produce the modulus value N.
2. Calculate the value of Euler expansion function Φ (N) :

$$\Phi\ (N) = (p-1)(q-1)(p+1)(p-1) \qquad (2)$$

3. The largest common divisor (GDC) of e and Φ (N) is 1, (1 < e < n) with formula :

$$GDC\ (e, \Phi\ (N)) = 1 \qquad (3)$$

4. Look for Least Common Multiple (LCM) of the Lehmer Totient function so that it is obtained:

$$R(N) = LCM\ (p-1, q-1, p+1, q+1) \qquad (4)$$

5. Then look for d value :

$$e\ x\ d\ \ Mod\ R(N) = 1 \qquad (5)$$

6. The value of e is the public key, while the value of d is the private key.

The encryption function of LUC algorithm is defined as follows :

$$V[i] = (\ M\ *\ V[i-1]\ -\ V[i-2])\ \ mod\ N$$

The encryption function will calculate the i-term of the Lucas line with the index i being the public key e and M being the plaintext.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023
DOI : https://doi.org/10.33395/sinkron.v8i2.12202
e-ISSN : 2541-2019
p-ISSN : 2541-044X

The decryption function of LUC algorithm is defined as follows :

$$V[i] = (C * V[i-1] - V[i-2]) \ mod \ N$$

The decryption function will calculate the i-term of the Lucas line with the index i being the private key d and C being the ciphertext.

Brute Force Attack

A brute-force attack involves trying every possible key until an intelligible translation of the ciphertext
into plaintext is obtained.[4] Brute force attack is a time-consuming attack due to the large sample space of possible keys that have to search. In this study, we will simulate attacks on ciphertext obtained from the aes key encryption process using the luc algorithm. The brute force attack is more focus on integer factorization that tries to factorize from the n value in public key. In the simulation, the adversary is given as the public key and ciphertext. The adversary will try to brute force all possible keys to decrypt the ciphertext.

RESULT

This research is a model of a combination of the AES cryptographic algorithm, and the LUC algorithm in a hybrid framework. The AES algorithm used is AES-128 which uses 10 rounds in the encryption and decryption process. The AES algorithm is used for data security, then the LUC algorithm is used for AES key security. To carry out the implementation of this research, the authors need to do analysis and trials.

Table 1. Estimated encryption and decryption time with the AES algorithm

Number of Characters	AES Encryption Time	AES Decryption Time
100	0.01848	0.01921
200	0.02473	0.02638
300	0.02924	0.02931
400	0.03988	0.04102
500	0.04545	0.04823

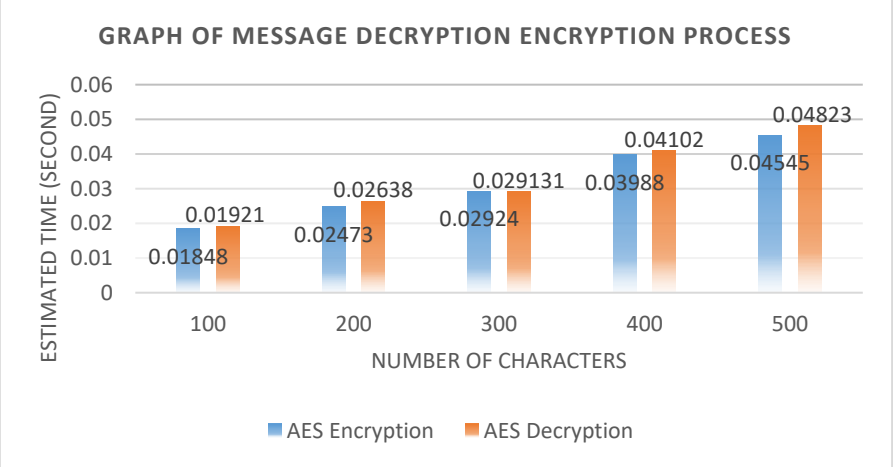

Figure 3. AES encryption and decryption time estimation

From the test results, the estimated time for encryption and decryption of the AES algorithm (with the number of different message characters experienced an increase in time, but the increase in time did

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023
DOI : https://doi.org/10.33395/sinkron.v8i2.12202
e-ISSN : 2541-2019
p-ISSN : 2541-044X

not experience much difference. The process of encrypting a message with 100 characters using AES produced a time of 0.01848 s, while a message with 500 characters produced a time of 0.04545 s. So with a difference of 400 message characters, the time difference is 0.02697 s or less than 1 second.

Table 2. Estimated encryption and decryption time combined with the AES algorithm and the LUC algorithm

Number of Characters	Encryption Time	Decryption Time
100	9.69445	0.05775
200	10.79356	0.06412
300	11.98359	0.06596
400	13.51866	0.08286
500	18.61569	0.08555

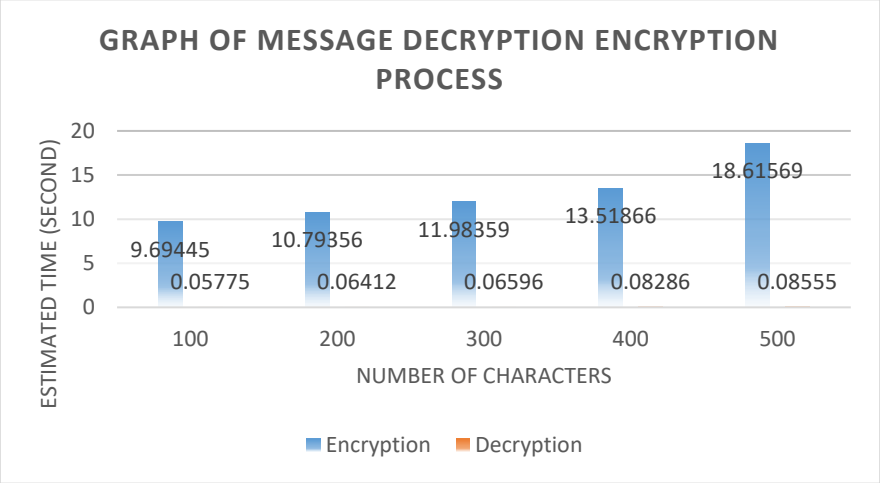

Figure 4. AES and LUC combined encryption and decryption time estimation

The time needed to carry out the encryption and decryption process with the combination of the AES and LUC algorithms will be longer when compared to carrying out the encryption and decryption process with the AES algorithm.

In this study a brute force attack simulation test was also carried out against the LUC algorithm. In contrast to the real world, in this simulation it is assumed that the algorithm used is known. The attack simulation is carried out by calculating the possibility of the private key (d) being used brute force with the help of the public key (e) and ciphertext which is publicly known.

```
Enter the ciphertext : 153 339 924 797 387 948 528 973 32 765 924 889 32 948 889 51

Cyphertext:  [153, 339, 924, 797, 387, 948, 528, 973, 32, 765, 924, 889, 32, 948, 889, 51]

LUC decrypting, Cyphertext: [153, 339, 924, 797, 387, 948, 528, 973, 32, 765, 924, 889, 32, 948, 889, 51]

Enter E key:367
Key tried: [153, 339, 924, 797, 387, 948, 528, 973, 32, 765, 924, 889, 32, 948, 889, 51]
Finding P,Q, N and D for this key....
Got the plaintext, LUC decrypt result:  S2INFORMATIKAOKE
Total combination searched: 451
Brute Force time:  70.32387661933899
LUC KEY: P=37, Q=29, N = 1073, d = 17743
```

Figure 5. Brute Force attack simulation process on the LUC Algorithm

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i2.12202 p-ISSN : 2541-044X

Table 3. The simulation results of the LUC Algorithm Brute Force attack

Public Key (E)	Brute Force Attack Time (second)	Result
367	70.3238	Private Key and Plaintext found
631	768.8782	Private Key and Plaintext found
743	1781.6294	Private Key and Plaintext found
977	52798.2548	Private Key and Plaintext found
1087	93287.3085	Private Key and Plaintext found

The brute force attack carried out against the LUC Algorithm was successfully carried out and the plaintext could be found. The greater the value of the E (Public Key) LUC Algorithm, the longer the brute force attack will take to find the plaintext.

DISCUSSIONS

The combination of the aes and luc algorithms will increase the computation time of the encryption and decryption processes that are carried out if compared to the computational time of the aes algorithm itself.

To test the luc algorithm which plays a role in securing the aes key, a brute force attack simulation was carried out by utilizing e as a public key to try several possible private keys d. To get the value of d (private key), that is by calculating the modular equation e*d mod R(N) = 1, where e is the known public key and R(N) is the most common multiples of p and q. The greater the value of n resulting from the addition of two prime numbers p and q the more difficult it is to guess the combination of values of the two prime numbers.

Likewise with the value of e, the greater the value of e that we use as the public key in the luc algorithm, the longer it takes to be able to do it violent attack. This is directly proportional to the encryption and decryption processing time of the luc algorithm itself.

CONCLUSION

Based on the analysis in the design and testing a combination of AES and LUC cryptographic algorithms to secure text, it can be concluded that the combination of AES and cryptographic algorithms LUC algorithm was successfully carried out. The time required for the combination of the AES and LUC algorithms to carry out the encryption and decryption process is longer when compared with the processing time of the AES algorithm.

The simulation results of the brute force attack performed show that the LUC algorithm can still be attacked. The greater the value of E (the public key of the LUC algorithm), the longer it takes for the brute force attack to be successful, but the value of E is also directly proportional to the computational time required by the LUC algorithm to carry out the encryption and decryption processes. So it can be concluded that the AES algorithm is less precise when combined with the LUC algorithm.

REFERENCES

[1] Mahmud, A. H., Angga, B. W., Tommy, Marwan, A. E., dan Siregar, R. 2018. Performance analysis of AES-Blowfish hybrid algorithm for security of patient

[2] Anane Nadjia and Anane Mohamed. 2015. AES IP for Hybrid Cryptosystem RSA-AES. 2015 12th International Multi-Conference on Systems, Signals & Devices

[3] Iavich, M., Gnatyuk, S., Jintcharadze, E., Polishchuk, Y., and Odarchenko, R. 2018. Hybrid Encryption Model of AES and ElGamal Cryptosystems for Flight Control Systems. *2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control, MSNMC 2018 - Proceedings*, 127–131.

[4] Stallings, W. 2017. Cryptography and Network Security Principles and Practices, Seventh Edition. Prentice Hall

*name of corresponding author

[5] Ritambhara., Alka Gupta., Manjit Jaiswal. 2017. An Enhanced AES Algorithm Using Cascading Method On 400 Bits Key Size Used In Enhancing The Safety Of Next Generation Internet Of Things (IOT). *International Conference on Computing, Communication and Automation (ICCCA2017)*

[6] Sari, P. P., Nababan, E. B., dan Zarlis, M. 2020. Comparative Study of LUC, ElGamal and RSA Algorithms in Encoding Texts. *MECnIT 2020 - International Conference on Mechanical, Electronics, Computer, and Industrial Technology*, 148–151.

[7] Mok, C. J., and Chuah, W. C. 2019. An Intelligence Brute Force Attack on RSA Cryptosystem.*Communications in Computational and Applied Mathematics, Vol. 1 No.1 (2019) p. 1-7.*

[8] Prameshwari, A., dan Sastra, N. P., 2018. Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *Jurnal Eksplora Informatika Vol. 8, No.2, September 2018.*

[9] Rachmawati, D., Sharif, A., Jaysilen, dan Budiman, M. A. 2018. Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm. *IOP Conference Series: Materials Science and Engineering*, *300*(1).

[10] Ramadani, D. 2018. Implementasi Algoritma LUC Dalam Penyandian Teks. *MEANS (Media Informasi Analisa Dan Sistem)*, *3*(1), 36–41.

[11] Rivera, L. B., Bay, J. A., Arboleda, E. R., Pereña, M. R., and Dellosa, R. M. 2019. Hybrid cryptosystem using rsa, dsa, elgamal, and aes. *International Journal of Scientific and Technology Research*, *8*(10), 1777–1781.

[12] Zulkarnain, M. A., and Nawara M. A. M. 2012. Computation of Private Key Based on Divide-By-Prime for Luc Cryptosystems. *Journal of Computer Science 8 (4): 523-527, 2012*

[13] Ruziq, F., Sihombing, P., and Sawaluddin. 2020. Combination Analysis of Data Encryption Standard (DES) Algorithm and LUC Algorithm on File Security. *International Journal of Research and Review. Vol.7; issue: 2; February 2020.*

[14] Winafil, M., Sinurat, S., dan Zebua, T. 2018. Implementasi Algoritma Advanced Encryption Standard Dan Triple Data Encryption Standard Untuk Mengamankan Citra Digital. *Komik (Konferensi Nasional Teknologi Informasi dan Komputer)* 2: 450–459

[15] Alegro, J. K. P., Arboleda, E. R., Perena, M. R., and Dellosa, R. M., Hybrid Schnorr, RSA, and AES Cryptosystem. *International Journal of Scientific & Technology Research Volume 8, Issue 10, october 2019.*

*name of corresponding author