# rid_Algorithm_and_AES_Advanced_Encryption_Standard_Algorithm.pdf

*by*

**Submission date:** 14-Jun-2022 08:48AM (UTC+0700)
**Submission ID:** 1856391577
**File name:** rid_Algorithm_and_AES_Advanced_Encryption_Standard_Algorithm.pdf (477.53K)
**Word count:** 4007
**Character count:** 21259

*Article*

# E-mail Security System Using El-Gamal Hybrid Algorithm and AES (Advanced Encryption Standard) Algorithm

**Jumadi Mabe Parenreng [1], Sahraeni Maulida [2], Abdul Wahid [3]**

[1]Department of Informatics and Computer Engineering, Faculty of Engineering, State University of Makassar,
[2]Department of Informatics and Computer Engineering, Faculty of Engineering, State University of Makassar,
[3]Department of Informatics and Computer Engineering, Faculty of Engineering, State University of Makassar

* Corresponding author: syahraenimaulidaida0600@gmail.com

**Abstract:** E-mail is a medium of long-distance communication via the internet, which is currently often used for message exchange needs. But the use of e-mail has security problems, especially regarding data leakage when sending messages via e-mail. One of the efforts to improve the security of data and information is the application of cryptographic techniques and methods, namely end-to-end encryption. Cryptography is the science of reducing the risk of security threats by encrypting and decrypting data and information. In the implementation of the e-mail system, at least 2 (two) suitable encryption techniques are needed, namely symmetric encryption techniques to encrypt messages and data to be sent via e-mail effectively and efficiently, and asymmetric encryption techniques used to distribute keys used by symmetric encryption. Therefore, in this study, we use the El-Gamal encryption model to distribute the symmetric key, and the AES encryption model is a fairly secure algorithm to protect message data or confidential information.

**Keywords:** Security, Email Security, El-Gamal Algorithm, AES Algorithm, Cryptography

check for updates

**Citation:** Parenreng J.M, Maulida.S, Wahid.A, E-mail Security System Using El-Gamal Hybrid Algorithm and AES (Advanced Encryption Standard) Algorithm. *Iota*, **2022**, ISSN 2774-4353, Vol.02, 01. https://doi.org/10.31763/iota.v2i1.510

Academic Editor : P.D.P.Adi

Received : 14 January 2022

Accepted : 05 February 2022

Published : 15 February 2022



## 1. Introduction

Electronic mail and the internet provide the means promising to conduct surveys in the future as the proportion of people accessible via e-mail or the internet continues to increase. It estimates that 45% of households now own a computer, and the proportion on the internet is 22% (Witt, 1997). E-mail surveys can be conducted faster than telephone surveys, especially for large samples, where the number of telephones and trained interviewers limits the number of completions per day. This method is inexpensive, as it eliminates postage, printing, and/or interviewer costs[1]. the use of e-mail to exchange information and collaborate is not only limited to public information but also confidential information, which has marked secrecy to parties certain so that need existing security. [2]

Problem security and confidentiality are essential aspects of messages, data, or information. Where is the truth and authenticity of something essential information good at the moment of the delivery or when information the accepted? Messages, data, or information will be useful again when delivery information is bugged or hijacked by people who aren't entitled or interested. [1] [3]

For it is indispensable something system security to guard secrecy information. one method used for objective the is cryptography with encrypting information sent because objective cryptography is confidentiality, integrity, and availability [4]. Encryption is a random process order order order no could read by people who don't entitle. scrambled

messages named ( ciphertext ) . for restoring message random ( ciphertext ) then message it's in the description, description is the process of returning message randomly, recovered messages named (plaintext). [5] [6]

Furthermore, Anticipate improving the security of messages, data, and information by implementing the El-Gamal algorithm in combination with the AES Algorithm. by combining the two algorithms, the level of security in the e-mail will be doubled.

## 2. Theory

### *2.1. Cryptography*

Cryptography comes from the Greek word Kryptos which means secret writing. No third party must interfere in a communication system consisting of a sender and a receiver of information. The purpose of cryptosystems is to keep intruders out of the sender-receiver exchange of information, which is done using encryption and decryption. So that cryptographic algorithms can implement messages in plaintext format combined with a key or to y. [1]

Cryptography is a process that deals with scrambles plaintext (plain text or clear text) into cipher text (a process called encryption), then back to plain text (known as decryption). The main feature of an asymmetric cryptographic system is the procedure of encryption and decryption done with two different keys public key and key personal. A private key cannot be derived with the help of a public key which provides a lot of strength for cryptographic security. [7] [8]

*Cryptography aim to give service security as follows:*

1. Confidentiality: The principle of confidentiality stipules that only the sender and the intended recipient can process message content. Confidentiality is Identical terms with confidentiality and privacy; there are many approaches to giving secrecy, from physical protection to algorithm mathematics that makes the data unintelligible. [ 1]
2. Availability: The availability principle states that resources should be available to authorized parties at all times.
3. Integrity: service that handles data changes that are not legitimate. To ensure data integrity, someone should own the ability to detect manipulation of data by parties who do not authorize it. Data manipulation includes things such as insertion, deletion, and substitution.[2] Integrity mechanisms ensure that the message content remains the same when it reaches its intended destination receiver as sent by the sender. [9] [10] [11]

*Cryptography divided Becomes two types:*

1. Secret Key Cryptography: When the same key is used for encryption and decryption, DES, Triple DES, AES, and RC5, may be examples of such encryption, then the mechanism is known as secret-key cryptography.
2. Public Key Cryptography: When two different keys are used, i.e., one key for encryption and another one for decryption, RSA, Elliptic Curve, and others may be examples of such encryption hence the mechanism is known as public-key cryptography. A number of an algorithm for the usual used for encrypting messages; several usual algorithms were used to encrypt a message, so the writer used the El-Gamal algorithm and AES Algorithm combined and made security on delivery of E-mail messages for security multiply double.

**Table 1. Comparison of symmetrical and Asymmetrical algorithms**

| No. | Algorithm | Algorithm features |
|---|---|---|
| 1 | El-Gamal Algorithm | 1. One key used to encrypt and encrypt data<br>2. Only use one key; this is a method more encryption simple<br>3. The length of the key used more small used for encrypting data, e.g., 128 bit<br>4. Provide performance more hurry and need more powerful computing than encryption asymmetric. |
| 2 | AES Algorithm | 1. Key pair used for encryption and description, key this known as a public key and key personal<br>2. Blessing of partner key, this is a more process complex<br>3. Encryption method asymmetric involve key more length, e.g., 1024 bit<br>4. Slower from encryption symmetrical and need power computing taller because the complexity |
| 3 | RSA Algorithm | 1. Security level algorithm RSA encoding is very dependent on the size key password ( in bits), because more big size key, then more big also possibility combination key that can be hacked with method check combination one by one key or more known with term brute force attack. If made something RSA password with 256 bits long, then the brute force attack method will Become no economic and vain if hackers don't feel willing/able to break through the password.<br>2. Security from system RSA cryptography is based on two math problems :<br>a) A problem in factorization number amount many<br>b) RSA problem, namely finds the modulo of the root en of a number composite n whose factor no is known. The password. |
| 4 | DES Algoritma | 1. have some superiority, namely the encryption process and description of the data simple and fast because the key is only in the form of number decimal 10 bit.<br>2. Long the key is too short, only 56 bits. With a long key, this type of attack tries all possibilities the key (brute force attack) becomes possible for conducted in time short. |

### *2.2. El- Gamal Algorithm*

The El-Gamal algorithm is algorithm key asymmetry based on the exchange Diffie-Hellman key for cryptography key public. Taher El-Gamal described this algorithm in 1985. This consists of problem logarithm discrete, algorithm sign hand, and encryption. The difference between the El-Gamal algorithm and RSA algorithm is RSA; security is based on finding factor numbers around big, while in the El-Gamal algorithm, security is based on the difficulty of calculating the discrete log of the large prime modulus. Another advantage of the El-Gamal cryptosystem is obtaining a different ciphertext every time you order or the same plaintext encrypted. Operation El-Gamal algorithm can be represented with three steps: stage generation key, stage encryption, and decryption. [12] [13] [14].

**Property El-Gamal Algorithm :**

1) **Number prime , p ( no secret )**
2) **Number random , g (g < p) ( no secret )**
3) **Random numbers. x (x < p) ( secret , private key )**
4) **$Y = g^x \bmod p$ ( no secret , public key )**

**5) m (plaintext) ( secret )**

**6) a and b ( ciphertext ) ( no secret )**

***6.1 Making keys***

Procedure for making key explained in steps following :

6.1.1 Choose any prime number p ( p can be shared between member groups)

6.1.2 Choose two fruit numbers random, g, and x , with conditions g < p and 1 xp – 2

6.1.3 Calculate $y = g^x \bmod p$ Result of this algorithm :

- Public key: triple ( y,g,p )
- Private key: pair ( x,p )

***6.2 Encryption Procedure***

The algorithm encryption procedure is explained in the following steps:

6.2.1 Arrange plaintext Becomes blocks m1, m2, … . , ( value every block inside interval [ 0, p-1].

6.2.2 Choose the random number k, which is deep Thing this is 1 kp – 2

6.2.3 Every block m encrypted with formula $a = g^k \bmod p$

$b = y^k m \bmod p$

the pair a and b is the ciphertext for block message m. therefore, a size ciphertext is twice the size of plaintext.

***6.3 Procedure Description***

Procedure algorithm description introduced in steps, with the following :

6.3.1 Use private key x for count $(a^x)^{-1} = a^{p-1-x} \bmod p$

6.3.2 Count plaintext m with equation : $m = b/a^x \bmod p = b(a^x)^{-1} \bmod p$

### 2.3 *AES (Advanced Encryption Standard Algorithm )*

The Advanced Encryption Standard ( AES ) algorithm is one of the algorithms for block cipher encryption published by the National Institute of Standards and Technology (NIST) in 2000. The purpose main of the algorithm is to replace the DES algorithm after appearing in several vulnerable aspects. NIST invites experts on encryption and data security worldwide to introduce innovative block cipher algorithms for encrypting and decrypting data with strong and complex structures. [1]

Many from all over the world send group algorithms to them. NIST accepts five algorithms for evaluation. After Doing various security criteria and parameters, they chose one of five algorithms encryption proposed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. The real name of the AES algorithm is the algorithm Rijndael. However, this name is not yet famous for algorithms but is recognized as Advanced Encryption Standard (AES) algorithms worldwide.[2]

AES is a system encoding non - Feistel blocks because AES uses components that always have an inverse with a long 128-bit block. AES keys use an iterative process called rounds. The processes in AES are transformations against states. A text original in block (128 bits) more formally organized as states. AES encryption is transformed to the state by repeated in a few rounds. The state that becomes the output of round k becomes the input for round -k +1; in the encryption process, at first original text is formed as a state.

Then before round 1 starts, block the text original mixed with the 0th round lock ( transformation this called AddRoundKey ). After that, the 1st round until with round-(Nr-1), where Nr is the number of rounds. [15]

AES uses four types of transformation, namely :

1. SubBytes , as transformation substitution.
2. ShiftRows , as transformation permutations.
3. MixColumns , as transformation randomization.
4. AddRoundKey , as transformation addition key. In the last round, i.e., the -Nr round is done, transformation similar to another round but without transformation MixColumns [16].

AES encoding requires a round lock for every round of transformation. The key to this round is raised( in expansion ) of the AES key. In part, this is discussed how the AES key generates the round lock. AES key 128 bit or four words produce an array of as many as 44 words that become key.

Moreover, The following is a step expand key :

1. First 128 bit AES key organized into 4 words and copied to the output word (W) on 4 elements first ( W[ 0], W[1], W[2], W[3]).
2. For element output then W[ i ] with i ={ 4,…,43} calculated as following
   a. Copy W[i-1] in word t.
   b. If i mod 4 = 0 ( I finished divided by 4) then do W[ i ]= f ( t,i ) W [i-4] , where the function f( t,i ) is as following : f( t, i ) = Subword ( rotword (t)) RC [ i /4]
   c. If I mod 4 doesn't same with 0, do W[ i ]= t W [i-4]. [16]

*2.4 Combination El-Gamal Algorithm and AES. Algorithm*

1. The sender determines the key to be sent to a recipient, which is encrypted using the El-Gamal algorithm. after the encrypted key, so will shape ciphertext.
2. The e-mail message sent to the recipient is encrypted using the algorithm AES after the encrypted e-mail message shapes ciphertext.
3. Ciphertext keys and E-Mail messages combined.
4. The ciphertext has been combined, then sent recipient.
5. Ciphertext until recipient, ciphertext key, and e-mail messages is separated.
6. Key in description more formerly use algorithm El-Gamal.
7. Then The E-mail message is described using a private key that has been described using El-Gamal.
8. The e-mail message is described using the AES algorithm.

## 3. Method

A method is an essential factor in determining the quality of research; other methods are used to regulate when the ad-hoc telecommunications process is submitted to previous research [20, 21, 22]. Furthermore, The Encrypt key uses the El-Gamal algorithm will give level multiple security double on message E-mail. In figure 1, the sender will send a message and key to the recipient; the key that has been made in encryption use El-Gamal Algorithm, then generates ciphertext from the key. Then the message is to be sent in encryption using the AES algorithm and generate a random message ( ciphertext). The ciphertext from the key and the message are merged and sent through e-mail. Next ciphertext that has been until the recipient is separated for described; key described use El - Gamal algorithm and message described with described key previously use AES algorithm. After describing so, the message can be read by the recipient.

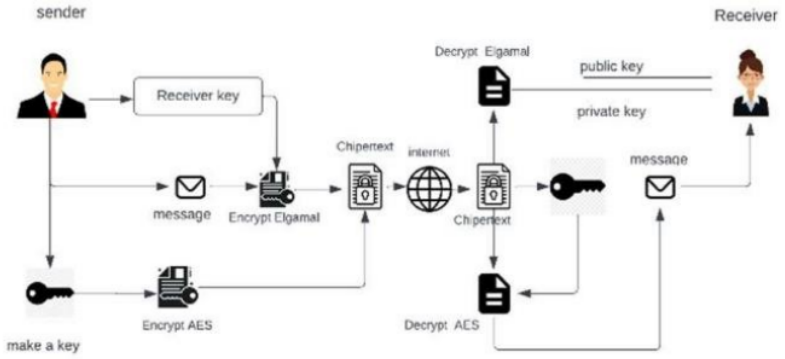


*Figure 1.* Design system

## 4. Result and Discussion

Implementation and experiment system on research this using the Python programming language. Needed two e-mail addresses used as sender and receiver. Test security and analysis from the study are done in two stages: in each algorithm, encryption and decryption in parallel. Encryption and description use algorithm ElGamal and AES algorithm.

Difficulty biggest for penetrating security from algorithm Elgamal is at on difficulty for To do calculation logarithm discrete. Where for could form a private key for the decryption process, then the intruder must solve the equation: y = gx mod p. Where should the intruder be looked for the x value of equality? Although the values of y, g, and p are known, finding the x value of equality the very difficult, especially if the p-value is a large prime number. Because of that, the bigger the prime number, the more difficult the x value is to find. Analysis testing security from algorithm Elgamal with technique gross force can be conducted with see probability combination existing key. _ Is known that: Public key = y, g, p (y, g, and p not secret ) Private key = x,p ( p is no secret, only x is secret ) Where conditions that must be fulfilled is g.

### *4.1 Encryption results*

On Step encryption, key and e-mail message sent in form ciphertext, encrypted message use algorithm Elgamal currently e-mail messages in encryption use algorithm AES and key in encryption use El-Gamal algorithm, key and message could see on image 2, on key public used key 12345 with results encryption **J6WcK7yFGGVkXaIOANtnSOWTosZnxCwKt EFNGEq6ZeU** =, i.e., ciphertext, and E-mail message with contents of "this" is the example message "with results Encryption "**J6WcK7yFGGVkXaIOANtnSOWTosZnxCw KtEFNGEq6ZeU=###vbd/TFYkiPXIDCLjxgk/kTMBfpV FUpb3cmqZ2qxs7/XW4OTYCnXBl+U3xQjc.**

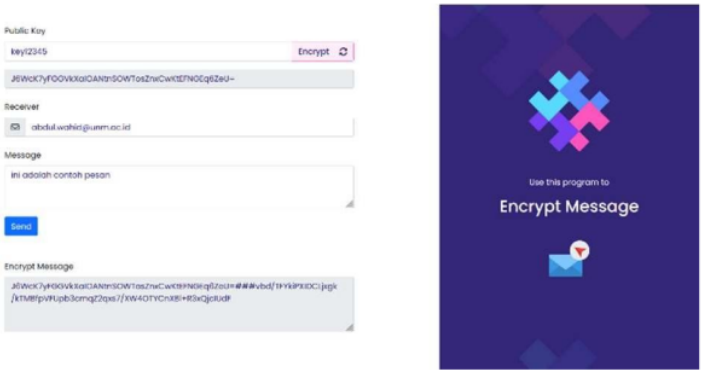


*Figure 2.* Encryption Results

### *4.2 Result Description*

In stages, this description of content e-mail messages and keys is symmetrical and put together in one display. What sets it apart is at the time, enter the following key needed for the decryption process. The decryption process can be seen in Figure 3.

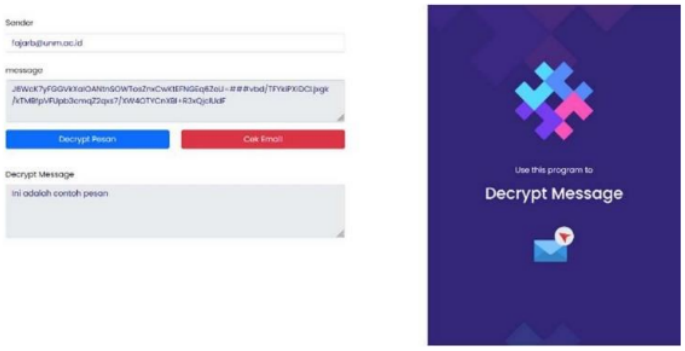


*Figure 2.* Description result

## 5. Conclusions and Suggestion

The use of E-mail for the exchange of information is not only limited to public information but also information confidentiality; for that study, this has To do with e-mail security by combining two algorithms, cryptography is ElGamal and AES for the encryption and decryption process. ElGamal used for secure key symmetrical ones will be used during the description process. In contrast, AES is used for secure message e-mail that will be sent. Study this has To do e-mail security with combine two algorithm cryptography that is ElGamal and AES for encryption process and description. ElGamal used for secure key symmetrical ones will use during the description process.

In contrast, AES is used for security. Contents of e-mail messages that will be sent. On algorithm, Elgamal large resource required because generated ciphertext twice the

length. Algorithm Elgamal is located on difficulty calculation logarithm discrete on a large prime modulo, so that effort for complete problem logarithm becomes challenging to solve. On the AES algorithm Method, encryption involves the key length and is slower and needs power computing taller because of the complexity.

**Author Contributions:** Conceptualization; Parenreng J.M (P.J.M), Maulida.S (M.S), Wahid.A (W.A) ; methodology; (P.J.M),(M.S),(W.A), validation; (P.J.M),(M.S),(W.A); formal analysis; (P.J.M),(M.S),(W.A); investigation; (P.J.M),(M.S),(W.A); data curation; (P.J.M),(M.S),(W.A); writing—original draft preparation; (P.J.M),(M.S),(W.A); writing—review and editing; (P.J.M),(M.S),(W.A); visualization; (P.J.M),(M.S),(W.A); supervision; (P.J.M),(M.S),(W.A); project administration (P.J.M),(M.S),(W.A); funding acquisition; (P.J.M),(M.S),(W.A); have read and agreed to the published version of the manuscript.

**Acknowledgments:** Sahraeni Maulida is Supported by The Department of Informatics and Computer Engineering, Faculty of Engineering, State University of Makassar.

**Conflicts of Interest**: The authors declare no conflict of interest.

## References

1. DR Schaefer and DA Dillman , "Development of a Standard E-Mail Methodology: Results of an Experiment," Public Opin . Q. , vol. 62, no. 3, p. 378, 1998, doi : 10.1086/297851.
2. International Conference on Advanced Communication Technology, Global IT Research Institute, IEEE Communications Society, and Institute of Electrical and Electronics Engineers,The 18th International Conference on Advanced Communication Technology: "Information and Communications for Safe and Secure Life": ICACT 2016 : Phoenix Park, Pyeongchang, Republic of Korea : Jan. 31 - Feb. 3, 2016 : proceedings & journals . 2016. Accessed: Jul. 19, 2021. [Online]. Available:http://ieeexplore.ieee.org/servlet/opac?punu mber=7415107
3. MR Bodkhe and V. Jethani , "HYBRID ENCRYPTION ALGORITHM BASED IMPROVED RSA AND DIFFIE-HELLMAN," Int. J. Eng. , vol. 4, no. 1, p. 15, 2015.
4. MAA Halim, CC Wen, I. Rahmi , NA Abdullah, and NH Ab. Rahman, "E-mail authentication using symmetric and asymmetric key algorithm encryption ," Kedah, Malaysia, 2017, p. 020047. doi : 10.1063/1.5005380.
5. V. Kapoor, "Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and 'n'prime Numbers," vol. 1, p. 4, 2013.
6. NY Goshwe , "Data Encryption and Decryption Using RSA Algorithm in a Network Environment," p. 5, 2013.
7. V. Kapoor and R. Yadav, "A Hybrid Cryptography Technique for Improving Network Security," Int. J. Comput . apps . , vol. 141, no. 11, pp. 25–30, May 2016, doi : 10.5120/ijca2016909863.
8. S. Nisha and M. Farik , "RSA Public Key Cryptography Algorithm – A Review," vol. 6, no. 07, p. 5, 2017.
9. "A SURVEY PAPER ON CRYPTOGRAPHY TECHNIQUES," Int. J. Comput . science . mobs . Computing . , vol. 5, no. 8, pp. 55–59, August 2016.
10. A. Chavan, A. Jadhav, S. Kumbhar , and I. Joshi, "Data Transmission using RSA Algorithm," vol. 06, no. 03, p. 3, 2019.
11. RS Jamgekar and GS Joshi, "File Encryption and Decryption Using Secure RSA," vol. 1, no. 4, p. 4, 2013.
12. F. Mallouli , A. Hellal , N. Sharief Saeed, and F. Abdulraheem Alzahrani , "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms," in 2019 6th IEEE International Conference on Cyber Security and Cloud Computing ( CSCloud )/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud ( EdgeCom ) , Paris, France, Jun. 2019, pp. 173–176. doi: 10.1109/ CSCloud /EdgeCom.2019.00022.

13. OA Imran, SF Yousif, IS Hameed, WN Al-Din Abed, and AT Hammid , "Implementation of El-Gamal algorithm for speech signals encryption and decryption," Procedia Computing . science . , vol. 167, pp. 1028–1037, 2020,doi : 10.1016/j.procs.2020.03.402.
14. SF Yousif , AJ Abboud , and HY Radhi, "Robust Image Encryption With Scanning Technology, the El- Gamal Algorithm and Chaos Theory," IEEE Access , vol. 8, pp. 155184–155209, 2020, doi : 10.1109/ACCESS.2020.3019216.
15. Chen JunLi , Qing Dinghu , Yu Haifeng , Zhang Hao , and MeiJuan Nie , "E-mail encryption system based on hybrid AES and ECC," in IET International Communication Conference on Wireless Mobile and Computing ( CCWMC 2011) , Shanghai, China, 2011, pp. 347–350. doi : 10.1049/cp.2011.0906.
16. AM Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," p. 13, 2017.
17. Castro, MC, Arboleda, ER, & Corpuz, RR (2019). Aes and merkle-hellman knapsack hybrid cryptosystem. International Journal of Scientific and Technology Research , 8 (12), 97–101
18. People, G. (1994). Cryptographic Algorithms and current trends. Netmode.Ntua.Gr , 1–13. http://www.netmode.ntua.gr/courses/postgraduate/edi/e rgasies2006/PSYLLOS_cryptography.pdf
19. Muhammad Abdullah, A., & Muhamad Abdullah, A. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data View project Call for papers View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt . June . https://www.researchgate.net/publication/317615794
20. Puput Dani Prasetyo Adi, et.al., "A Study of Programmable System on Chip (PSoC) Technology for Engineering Education", October 2020, Journal of Physics: Conference Series, Volume 1899, 2nd Workshop on Engineering, Education, Applied Sciences and Technology (WEAST) 2020 5 October 2020, Makassar, Indonesia, doi:10.1088/1742-6596/1899/1/012163
21. P. D. P. Adi and A. Kitagawa, "Performance Evaluation of Low Power Wide Area (LPWA) LoRa 920 MHz Sensor Node to Medical Monitoring IoT Based," 2020 10th Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS), 2020, pp. 278-283, doi: 10.1109/EECCIS49483.2020.9263418.
22. M. Niswar et al., "Performance evaluation of ZigBee-based wireless sensor network for monitoring patients' pulse status," 2013 International Conference on Information Technology and Electrical Engineering (ICITEE), 2013, pp. 291-294, doi: 10.1109/ICITEED.2013.6676255.

rid_Algorithm_and_AES_Advanced_Encryption_Standard_Alg...

ORIGINALITY REPORT

| 8% | 4% | 6% | 3% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

1%

★ Yuanyu Chen, Shauchun Wang. "Development of Coplanar Electro-Wetting Based Microfluidic Sorter to Select Micro-Particles in High Volume Throughput at Milliliter Amount within Twenty Minutes", Sensors, 2018

Publication

| | | | |
|---|---|---|---|
| Exclude quotes | Off | Exclude matches | Off |
| Exclude bibliography | On | | |

# rid_Algorithm_and_AES_Advanced_Encryption_Standard_Algori

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

**Instructor**

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9