Edu Komputika 9 (1) (2022)

Edu Komputika Journal

http://journal.unnes.ac.id/sju/index.php/edukom

Comparative Study of RSA Asymmetric Algorithm and AES Algorithm for Data Security

Siti Alvi Sholikhatin✉, Adam Prayogo Kuncoro, Afifah Lutfia Munawaroh, dan Gilang Aji Setiawan

Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto, Indonesia

Info Artikel

Sejarah Artikel:
Diterima: Juni 2022
Direvisi: Januari 2023
Disetujui: Januari 2023

Keywords:
Data security, RSA Algorithm, AES Algorithm, Encryption, Cryptography

Abstrak

There are many ways to ensure data security, one of the classic way but still effective is to use encryption. Encryption itself has two techniques or algorithms: symmetric-key (also called secret-key) and asymmetric-key encryption (also called public key). In this paper, we proposed an analysis of two algorithm of encryption: RSA and AES algorithm in term of securing digital data. The method used in this research are: RSA and AES analysis, then retrieving the result. The two algorithm is deeply and thoroughly analyzed to discover the effectiveness to secure the data. The Technological Readiness Level (TKT) is at level 6, which means demonstration of a model or prototype or the analysis result of a system or subsystem or a study in a relevant environment. The result concluded that the application of the AES encryption algorithm is more optimal than RSA encryption in digital data security. Because the encryption and decryption process of using the AES algorithm is faster, although the difference in testing time of the two encryption algorithms is not too significant. The entropy value of 4.96 in AES encryption is greater than that of RSA proving that the even distribution of characters in the chiper text code does not accumulate on certain characters so that it will be difficult to attack using frequency analysis.

✉ Alamat korespondensi:
Jl. Letjend Pol. Soemarto No.127, Watumas, Purwanegara, Kec.
Purwokerto Utara, Kab. Banyumas, Jawa Tengah 53127
E-mail: alvi.sholikhatin@gmail.com

ISSN 2252-6811
E-ISSN 2599-297X

INTRODUCTION

Data security is an emerging issue that has been addressed nowadays in many field. Data has important role so to maintain its security is a top tier requirement. In this digitalized era where data could be accessed everywhere and anytime, providing secure data to the users also includes providing security during data transfer and the data storage (Akhil et al., 2018). People acquire security by making their data very confidential (Amalarethinam & Leena, 2017). One of many ways to secure data is using encryption. Encryption is the process of encrypting data so that it cannot be read by doing various substitutions and transformations in plaintext (original message) and converting them into cipher-text (random messages) (Simarmata et al., 2018). By applying encryption into the data or information, the security of it can be increased from potential attacks by third party or unauthorized access. Encryption also can be one of the way to maintain the confidentiality, availability, and integrity of the data itself.

Encryption algorithms are grouped into two general categories: Symmetric-key (also called secret-key) and asymmetric-key encryption (also called public key). The symmetric cryptography used the same key for encryption and decryption data, while the asymmetric cryptographic relies on two different keys for encryption and decryption (Muhammad Abdullah & Muhamad Abdullah, 2017). In this research, researcher is conducting a comparative analysis on two algorithms: Advanced Encryption Standards (AES) and RSA algorithm.

RSA is the most widely used key cryptography algorithm and was proposed by Rivest, Shamir and Adleman in 1977. In the RSA encryption algorithm, both public and private keys can be used to encrypt data and can guarantee that the private key can't be derived from the public key (Xu et al., 2020). AES algorithm is symmetrical block cipher that can encrypt and decrypt data, and is an iterative block cipher that has been chosen by the NIST (National Institute of Standards and Technology) as the international standard and replacement for DES (Lytvyn et al., 2019). The two algorithm is deeply and thoroughly analyzed to discover the effectiveness to secure the data.

The related previous research is the paper by Ye Yuan (Yuan et al., 2018) who conducted a high performance encryption system based on AES is proposed, in which AES can work at all three modes including AES-128, AES-192, and AES-256. In addition, AES implementation is piped into 4 stages for each round operation with decryption module reusing some circuits of encryption module, which leads to a performance improvement in term of area and throughput.

The research by Ünal Çavusoglu (Çavuşoğlu et al., 2017) who conducted a hybrid implementation of RSA algorithm using a novel chaos based RNG. This paper aims an encryption algorithm that combines the strong of asymmetric encryption algorithm and the rich dynamic behaviors of chaotic systems is developed. In this study, firstly a new chaotic system design with high dynamic features is performed and then circuit realization and analyses are made. A chaos based RNG (random number generator) is designed with the help of the new developed chaotic system, NIST and FIPS tests are run. Chaos based hybrid RSA (CRSA) encryption algorithm design in which RNG and RSA algorithms are used together is performed.

The comparative study also has been conducted by Santhosh Kumar B J (Santhosh Kumar et al., 2018) who analyzed the comparative study of RSA and AES algorithm for medical images. By considering different attacks on medical images by intruders, this paper suggests a few techniques which gives integrity to the image. The objectives of this paper is to compare two techniques (RSA, AES) which is used for encryption. By comparing these two methods the system will provide a more efficient in authentication and confidentiality.

An optical image compression and encryption scheme based on compressive sensing and RSA public-key cryptographic al- gorithm is proposed to enhance the security of image encryption system, where the optical compressive imaging system is utilized to sample the original image. This research is conduced by Lihua Gong (Gong et al., 2019). The results show the effectiveness and reliability of the proposed optical image compression and encryption scheme with considerable compression and security performance. The image encryption method also been conducted by Alireza Arab (Arab et al., 2019) with AES algorithm to encrypt image data.

The modification of RSA algorithm by Deepika Gupta (Mathur et al., 2017) is conducted to enhanced the level of security. The paper modified traditional RSA algorithm by including exponential powers, n prime numbers, multiple public keys, and K-NN algorithm. Modified approach also gives feature of verification at both side's sender and receiver. The last related researches are performed by Muhammad Fadlan (Muhammad Fadlan et al., 2021) and Septia Ulfa (Sunaringtyas & Prayoga, 2021) with the implementation of data security by using super encryption and penetration testing execution standard.

The goal of this research is mainly to determine which algorithm has significant impact on securing data by using encyption method. Both algorithm is widely used and are well known for their reliable encryption to protect data. The Technological Readiness Level (TKT) is at level 6, which means the demonstration of a model/prototype or the analysis result of a system/subsystem or a study is in a relevant environment. The two algorithm has been tested and implemented into the selected system in a certain organization in order to understand the effectiveness of both algorithms to secure data.

RESEARCH METHOD

RSA is a public key cryptographic technique to protect data from attacks. RSA can be used for encryption, key exchange (private and public key), digital signature. RSA is designed by Ron Rivest, Adi Shamir, and Leonards in 1978. RSA algorithm is very commonly used in data encryption and digital signature applications (Çavuşoğlu et al., 2017). In RSA any person can encrypt the data but for decryption it can be only done by the authenticated receiver. This encryption relies on cryptographic algorithm. In this paper, the data is being analyzed using RSA formula;

Encryption:
C = ME mod (N1)
Decryption:
M = CD mod (N2).

RSA algorithm is ilustrated in this Figure 1 below.

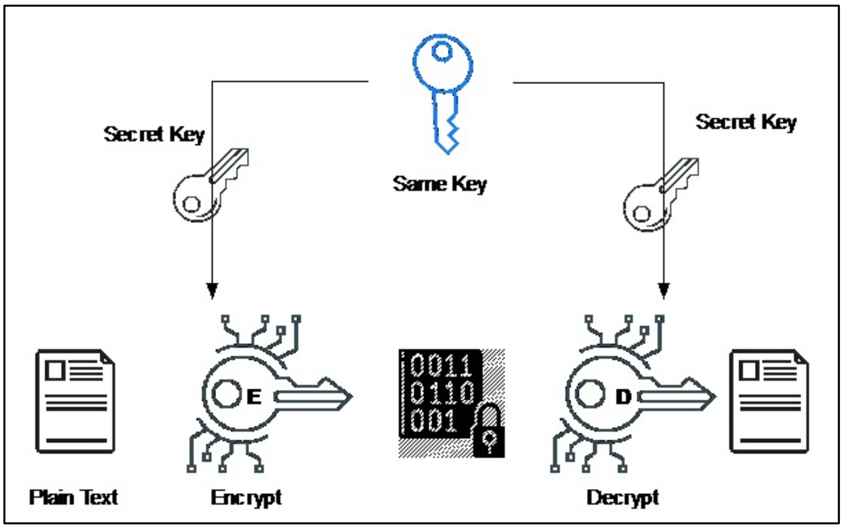


Figure 1. encryption process of RSA algorithm

AES based on Substitution Permutation Network. Using the technique, the host can encrypt and decrypt the data and they can keep their data safe. AES encompasses three block ciphers, AES-128, AES-192 and AES-256. AES is an iterative block cipher that has been selected by the NIST (National Institute of Standards and Technology) as the international standard (Lytvyn et al., 2019). All cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Secret-key ciphers use the same key for encoding and decoding the data, so both the sender and the receiver must know and use the same secret key. AES algorithm is ilustrated in this Figure 2 below.

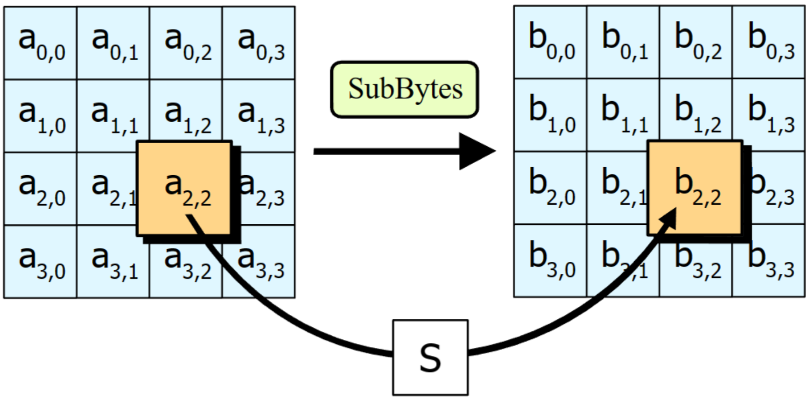


Figure 2. Substitution technique of AES algorithm

In this paper, the two encryption algorithm is compared to have a results of both effectiveness to secure data. The research flow can be seen in Fig. 1

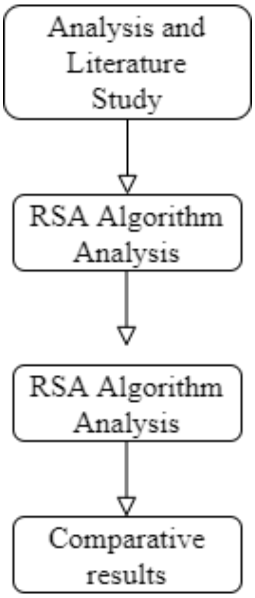


Figure 1 Research flow

Analysis and literature study is done to analyze the previous related researches. RSA algorithm and AES algorithm is done separately and to compare the effectiveness of the two method to secure digital data.

RESULTS AND DISCUSSION

Analysis and literature study have been conducted to give an overall understanding on the two algorithms from previous researchers. The first literature is guided by Deepika Gupta who proposed modified RSA to enhanced data security and super encryption. This research gives positive insight that RSA is considered effective to be implemented in data security. The second literature of comparative study on RSA and AES also held by Santhosh Kumar B J who concluded that both algorithms provide a more efficient in authentication and confidentiality of data security. The last literature is conducted by Ünal Çavusoglu who conducted a hybrid implementation of RSA algorithm using a novel chaos based RNG. Chaos based hybrid RSA (CRSA) encryption algorithm design in which RNG and RSA algorithms are used together is performed.

The research is focused on the comparation of assymetrical RSA and AES algorithm for digital data security. We conducted the test on digital signature in a web-based application. The design of application is built prior to the test for development research. The features include are certificate data input, signature process and verification of autenthicity.

1. Digital signature process

The initial process starts by inputting the plaintext first, the plaintext is first taken the message digest using the SHA-3 function. Then the message digest is processed by RSA and generates a ciphertext. Furthermore, the chiper text from the RSA are reprocessed by AES, produced the chiper text again and stored.

The encryption process by combining two cipher algorithms to produce text chiper results that are difficult to crack, first by entering the plaintext and then processing with the RSA algorithm to produce a text cipher, then the text chiper is processed again by AES and produces a text chiper and directly saved to the available database.

The data that needs to be entered are the data listed on the certificate, namely the certificate number, the name of the participant who will receive the certificate, the name of the activity or course, the name of the certificate ratifying official and the date the certificate was issued. An example of the two-stage encryption process can be seen in Table 1 below:

Table 1. Encryption result and QR code

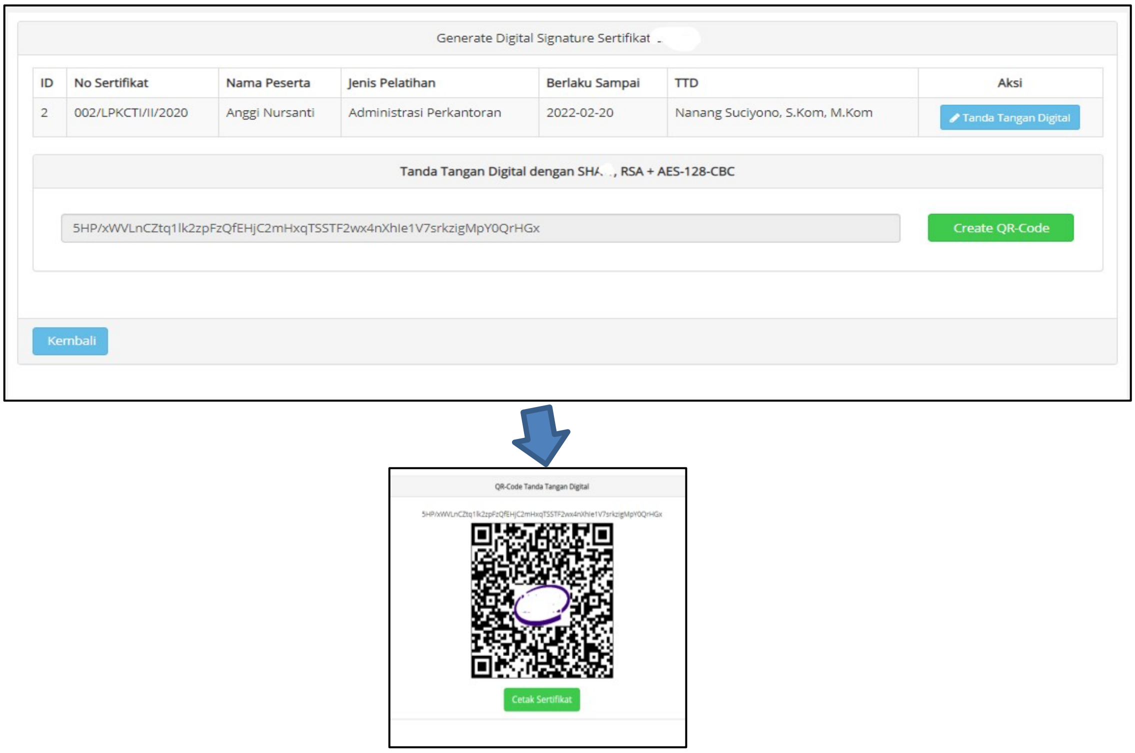
Certificate	Certificate number: 001/SERTIFIKAT/IF/V/2022 Name: Bagus Prasetyo Nugroho Type of training: Workshop Keamanan Data Digital Ratifier: Dr. Eng. Imam Tahyudin, M.M. Date issued: 10 Mei 2022
Plaintext	001/SERTIFIKAT/IF/V/2022| BagusPrasetyoNugroho| WorkshopKeamananDataDigital| 01/05/2022|
Message Digest (SHA-3)	5f4d45f0eabfd403b8b0416a6f310ebf5bf213d953821e000eec3c1123a71e6b (512 bit)
Super-encryption: - RSA - AES-128-CBC	MIsipjlgP3kHVc/rWRtN03v7HnMZRWaX94U+7fCv8vx/Euej0LHcQdBcCmMB5/4PVbDd Zn3eNt7d61qL6FeqDUxD9teFUNGqenc A46CLaJtSNinzt0HReZVe92O/VKFy (1024 bit)
QR code	

2. System architecture

This application has 2 main processes, namely: 1) input the certificate data in which the process of creating a digital signature code and QR-Code is carried out; and 2) the verification process by reading the QR-Code, inputting data on the certificate and matching the data according to the original digital signature code hidden behind the QR-Code.

This web-based digital signature application has a login procedure for users who will use it. The user here is an officer appointed by the digital certificate issuer to manage certificate data, create electronic certificates to send the certificate via email to each participant of the activity.

For the series of digital signature turning processes, the user selects the certificate data, then processes the creation of a digital signature code. After the code is obtained, enter the process of generating a QR-Code, then select print an electronic certificate. In detail, it can be seen in Figure 3 below.



Generate Digital Signature Sertifikat

ID	No Sertifikat	Nama Peserta	Jenis Pelatihan	Berlaku Sampai	TTD	Aksi
2	002/LPKCTI/II/2020	Anggi Nursanti	Administrasi Perkantoran	2022-02-20	Nanang Suciyono, S.Kom, M.Kom	Tanda Tangan Digital

Tanda Tangan Digital dengan SHA , RSA + AES-128-CBC

5HP/xWVLnCZtq1lk2zpFzQfEHjC2mHxqTSSTF2wx4nXhle1V7srkzigMpY0QrHGx

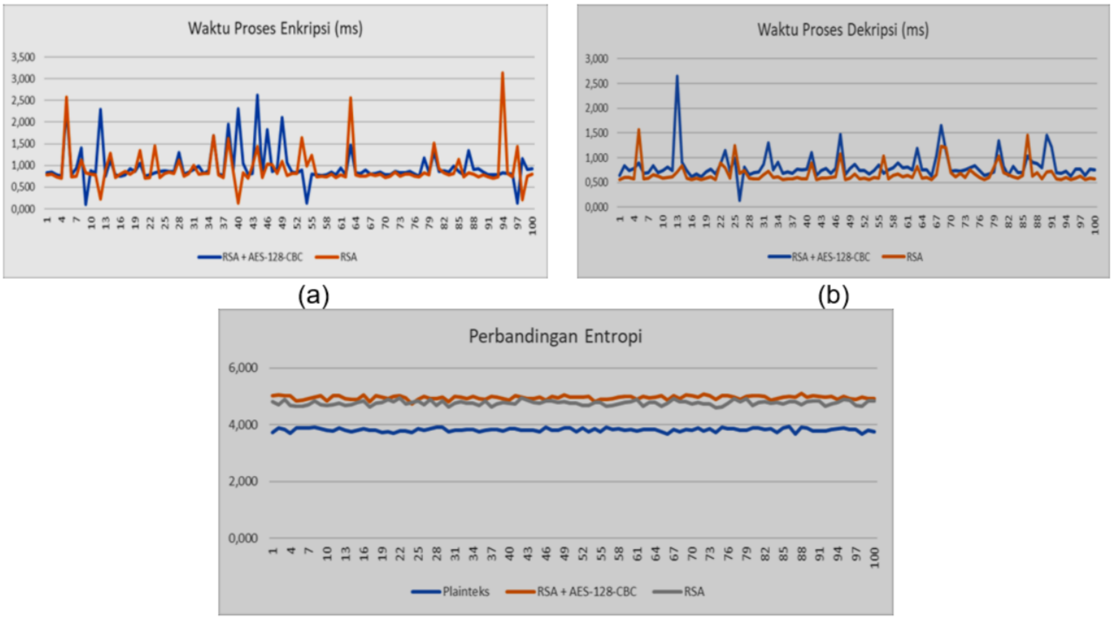
QR-Code Tanda Tangan Digital

5HP/xWVLnCZtq1lk2zpFzQfEHjC2mHxqTSSTF2wx4nXhle1V7srkzigMpY0QrHGx

Figure 3. The process of creating a digital signature.

3. Quality test of RSA and AES encryption

Testing was carried out on a sample of 100 digital signature certificate data, measuring the encryption process time, decryption process, entropy value, and the value of the avalanche effect described in Figure 3 below.



(a)

(b)

(c)

Figure 4. A comparison graph of encryption quality between the implementation of RSA cryptography and AES cryptography (the red line is the RSA algorithm, and the blue line is the AES algorithm)

Encryption quality testing is seen in terms of the speed of the encryption and decryption process, as well as the entropy value of the chiper text. The cryptographic system for digital signatures that only uses RSA compared to AES cryptography can be seen in Figure 3 (a) above, experiments were carried out on 100 plain texts with different file size obtained an average RSA encryption processing time of 0.92 milliseconds while AES encryption was found to be 0.96 milliseconds. With a difference of 0.04 milliseconds it will not be so pronounced, so the quality of this AES encryption can be declared more optimal. Likewise, with the decryption process time based on Figure 3 (b), the average result obtained from the RSA algorithm is 0.67 millisecon and the average result of the decryption time of AES encryption is 0.83 milliseconds, with a difference of 0.16 milliseconds. So that the decryption quality of this AES algorithm can be declared more optimal. Meanwhile, the results of the entropy assessment, from Figure 3 (c) above, can be determined that the entropy value of the chiper teks encryption resulting from the AES encryption of 4.96 is superior to the chiper text entropy resulting from RSA 4.77. The ideal entropy value is close to the number 8 thus the encryption system is designed to be secure from attacks (Irfan, 2016).

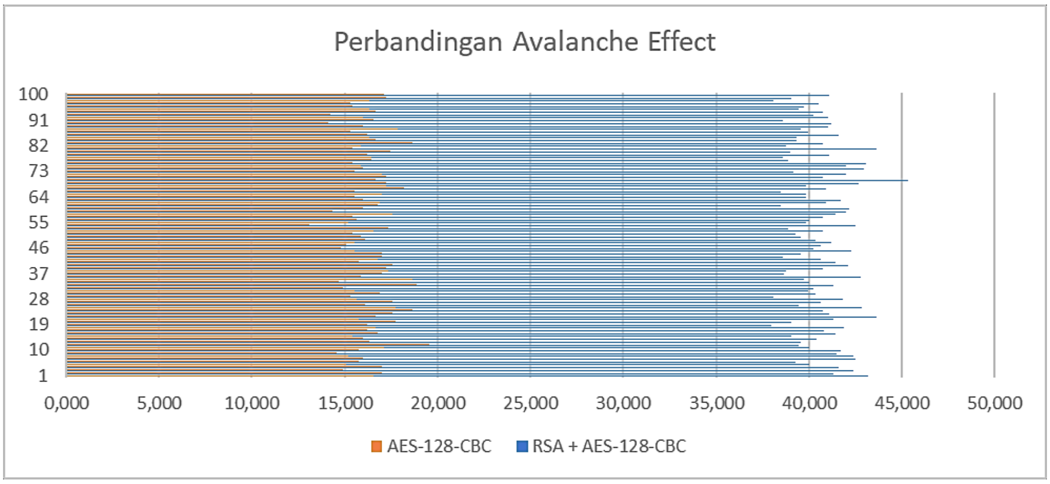


Figure 5. Comparison graph of quality of RSA encryption and AES encryption

Figure 4 shows the results of the avalanche effect testing on the AES encryption process and AES encryption. The plain text used to test the avalanche effect in determining the number of revolutions to be used in the encryption process, the number of character bits change from the initial plaintext to the new plaintext results in 1 bit of change only. Avalanche effect testing is performed to find out how much influence plain text changes have on chuoer text typically used in chiper block cryptographic systems such as AES. Visually from the tests carried out, the avalanche effect improvement of RSA encryption was generated with an average value of 16.31% while the avalanche effect of AES encryption obtained results with an average value of 40.61%. From the data from the test results, it can be concluded that the avalanche effect value of the AES encryption test is better than the RSA, based on the value of the avalanche effect close to 50%.

CONCLUSION

Based on the results of the research conducted, it can be concluded that the application of the AES encryption algorithm is more optimal than RSA encryption in digital data security. Because the encryption and decryption process of using the AES algorithm is faster, although the difference in testing time of the two encryption algorithms is not too significant. The entropy value of 4.96 in AES encryption is greater than that of RSA proving that the even distribution of characters in the chiper text code does not accumulate on certain characters so that it will be difficult to attack using frequency analysis. The avalanche effect value of 40.61% proves that the change in the chiper text code is already very random.

ACKNOWLEDGEMENT

The authors would like to thank LPPM of Universitas Amikom Purwokerto for the material and moral support so this research could be finished on time.

REFERENCES

Akhil, K. M., Kumar, M. P., & Pushpa, B. R. (2018). Enhanced cloud data security using AES algorithm. *Proceedings of 2017 International Conference on Intelligent Computing and Control, I2C2 2017*, *2018-Janua*, 1–5. https://doi.org/10.1109/I2C2.2017.8321820

Amalarethinam, I. G., & Leena, H. M. (2017). Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud. *Proceedings - 2nd World Congress on Computing and Communication Technologies, WCCCT 2017*, 172–175. https://doi.org/10.1109/WCCCT.2016.50

Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. *Journal of Supercomputing*, *75*(10), 6663–6682. https://doi.org/10.1007/s11227-019-02878-7

Çavuşoğlu, Ü., Akgül, A., Zengin, A., & Pehlivan, I. (2017). The design and implementation of hybrid RSA algorithm using a novel chaos based RNG. *Chaos, Solitons and Fractals*, *104*, 655–667. https://doi.org/10.1016/j.chaos.2017.09.025

Gong, L., Qiu, K., Deng, C., & Zhou, N. (2019). An optical image compression and encryption scheme based on compressive sensing and RSA algorithm. *Optics and Lasers* *in Engineering*, *121*(March), 169–180. https://doi.org/10.1016/j.optlaseng.2019.03.006

Irfan, P. (2016). Aplikasi Enkripsi Citra Menggunakan Algoritma Kriptografi. *Jurnal Matrik*, *16*(1), 96–104.

Lytvyn, V., Peleshchak, I., Peleshchak, R., & Vysotska, V. (2019). Information Encryption Based on the Synthesis of a Neural Network and AES Algorithm. *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings*, 447–450. https://doi.org/10.1109/AIACT.2019.8847896

Mathur, S., Gupta, D., Goar, V., & Kuri, M. (2017). Analysis and design of enhanced RSA algorithm to improve the security. *3rd IEEE International Conference On* , 3–7. https://doi.org/10.1109/CIACT.2017.7977330

Muhammad Abdullah, A., & Muhamad Abdullah, A. (2017). *Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Call for papers View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt*. https://www.researchgate.net/publication/317615794

Muhammad Fadlan, Haryansyah, & Rosmini. (2021). Pengamanan Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(6), 1113–1119. https://doi.org/10.29207/resti.v5i6.3566

Santhosh Kumar, B. J., Roshni, R. V. K., & Nair, A. (2018). Comparative study on AES and RSA algorithm for medical images. *Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, ICCSP 2017*, *2018-Janua*, 501–504. https://doi.org/10.1109/ICCSP.2017.8286408

Simarmata, J., Limbong, T., Ginting, M. B. R., Damanik, R., Nasution, M. I. P., Hasugian, A. H., Mesran, M., Sembiring, A. S., Hutahaean, H. D., Taufik, I., Hasugian, P. M., Sihotang, H. T., Gea, A., Hutapea, M. I., Jaya, I. K., Hasibuan, D., Situmorang, A., Naibaho, J. F., Napitupulu, J., … Sinambela, M. (2018). Implementation of AES Algorithm for information security of web-based application. *International Journal of Engineering and Technology(UAE)*, *7*(3.4 Special Issue 4), 318–320.

Sunaringtyas, S. U., & Prayoga, D. S. (2021). Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada. *Edu Komputika Journal*, *8*(1), 48–56.

Xu, Y., Wu, S., Wang, M., & Zou, Y. (2020). Design and implementation of distributed RSA algorithm based on Hadoop. *Journal of Ambient Intelligence and Humanized Computing*, *11*(3), 1047–1053. https://doi.org/10.1007/s12652-018-1021-y

Yuan, Y., Yang, Y., Wu, L., & Zhang, X. (2018). A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation. *2018 IEEE International Conference on Electron Devices and Solid State Circuits, EDSSC 2018*, 4–5. https://doi.org/10.1109/EDSSC.2018.8487056