Comparative Performance of Digital Signature Security Using Cryptography AES 192 BIT and RSA 512 BIT Algorithm Model

Dinda Husnaa Dhiyaulhaq [1*], Sahda Armandiva Usman [1]

[1]Department of Computer Science, Faculty of Mathematics and Natural Sciences, Universitas Negeri Semarang, Semarang, Indonesia
*Corresponding author: dindahusnaa30@students.unnes.ac.id

ARTICLE INFO

Article history
Received 7 August 2020
Revised 22 September 2020
Accepted 14 October 2020

Keywords
Cryptography
Digital Signature
Encryption
AES
RSA

ABSTRACT

Digital signatures are proof of authenticity and have the same function as a signature on a printed document, but the implementation is on digital documents. Public key cryptography or asymmetric keys are widely used in the implementation of data security on information and communication systems. The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and widely used public-key cryptography because of its less complexity. RSA has two main functions, namely the process of encryption and decryption process. This research was made to find out an explanation and discussion of the optimal algorithm for the performance of digital signature data security by comparing the performance of the RSA 512 bit and AES 192 bit algorithms with this, which is expected to provide knowledge about the security performance of digital signatures which in the future can be further developed in order to obtain security.

1 Introduction

The rapid development of technology cannot undeniably has changed the works of various activities in human life. In the present era, the need for communication is very large. One type of communication that humans use is visual communication. Especially in the current Covid-19 situation, human activities are limited and need technology. For example, if someone needs to sign an important letter and at that time, a power of attorney for signing is not present at the office because they work at home. This certainly overwhelmed some people, or it took a long time to get an autograph. A signature is a unique character that shows authentic proof of a printed document sent to the message's recipient.

As a solution, currently using a digital signature and its legality is recognized. A signature, digital marking, or digital signature have the same function, but the scope of their use is in digital documents. The process of procuring goods or services in a company sometimes involves documents that store private information in nature, such as source documents or the nominal price of goods listed. In addition, a signature is used as a tool to show the authenticity and validity of the document. When the documents are sent via the internet network, it is necessary to confirm who sent the documents and whom they will be sent (Menezes *et al.*, 1996).

There are several forms and kinds of threats to information, such as wiretapping, theft, falsification of information, and information misuse. With current technological developments, information exchange between parties is dispensable. Suppose the security of the exchange of information cannot be safeguarded. In that case, other parties may take advantage of the information so that it will harm the parties entitled to the information. Cryptography is one of the existing and appropriate solutions to maintain confidentiality and authenticity of data. Cryptography is the art or science to encode or encrypt a message so it can only be seen by people who have the decryption key.

Of the many public-key cryptographic algorithms that have been made, the most popular algorithm is the RSA algorithm (Ariyus, 2015). The RSA algorithm uses a public key and secret key to encrypt data, where the public key can be known by certain parties to decrypt data.

Based on this background, we need a digital signature security performance for confidentiality, data authenticity, and increased security on transaction data by using the RSA 512 bit algorithm and AES 192 bit.

Therefore, this study focuses on the AES and RSA algorithms' security performance on text encryption by making modifications to the AES and RSA algorithms. This study will use the performance comparison of the 512 bit RSA algorithm and the AES 192 bit algorithm. We use RSA because the RSA algorithm has a fairly good capability. It has a 2-way authentication key, namely a public key and a private key, so that it is safer in terms of maintaining security. Meanwhile, the AES 192 algorithm said it has a better security level because more encryption loops are making it difficult to read data. This paper also studied how to design, build, and implement 512 bit RSA and AES 192 bit algorithms in digital signature security for data security performance.

This paper aims to provide knowledge about the security performance of digital signatures using the RSA and AES cryptographic algorithms by comparing the performance of the two cryptography, which can be further developed in order to obtain more security. Also, to provide an overview of authentication and verification of digital documents using digital signatures to ensure the validity and confidentiality of these documents.

2 Literature Review

2.1 Computer Network

A computer network is a set of interconnections of a number from an autonomous computer. In popular language, it can be explained that a computer network is a collection of several computers that are connected to each other through an intermediate medium.

2.2 Data Security on Computer Networks

Network security is a collection of designed tools to protect data when transmitting against threats of access, alteration, and blocking by unauthorized parties (Sadikin, 2015).

2.2.1 Network Security Service

International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) defines several types of services and network security mechanisms. Network security services are defined based on the requirements that must be provided to meet the demand for network security.

2.2.2 Network Security Mechanism

In order to realize developer network security services system, we can use network security mechanisms. ITU-T (X.800) defines several network security mechanisms. The following are several types of network security mechanisms.

1. Encipherment (encoding)

   Encipherment is a network security mechanism used to hide data. Mechanism encipherment can provide data confidentiality services (Confidentiality), although it can also be used for other services. To realize the mechanism encipherment, cryptographic and steganographic techniques can be used. Things to know, cryptography is a collection of techniques to hide messages into hidden messages. Meanwhile, steganography is a collection of techniques for hiding messages on other media, such as pictures, sounds, or videos.

2. Data integrity

   Data integrity mechanisms are used to ensure data integrity in a data unit or on a stream data unit. The method used is to add test scores *(check value)* on the original data. So, when data are sent, the test score is calculated first, and then the data and examiners are sent together. The recipient

can test whether there is a change in data or not by calculating the test value of the data sent and comparing the calculated test value with the test value that was sent along with the original data. If the same, the recipient can conclude that the data has not been changed.

3. Digital signature

   The digital signature is a network security mechanism that provides a way for data senders to "electronically sign" a piece of data, and recipients can verify that "signature" electronically. Digital signature added to the data unit and used as proof of source sender and avoid counterfeiting (forgery) signature.

4. Authentication exchange

   This mechanism provides a way for two entities to authenticate each other by exchanging messages to prove each other's identity.

5. Traffic padding

   Traffic padding provides a way to prevent data traffic analysis on the network by adding fake data to data traffic.

6. Routing control

   Routing control provides a way to select and continuously change routes on the computer network between sender and receiver. This mechanism prevents communication from eavesdroppers.

7. Notarization

   Notarization (notarization) provides a way to select a trusted third party to control the communication between sender and receiver.

8. Access control mechanism

   Access control mechanisms provide a way for users to access data access to data, for example, with a Table of user relations and their authority (ability to access).

2.3 Cryptography

Cryptography is a study of securing information techniques. Security in cryptography can be guaranteed through four security services, namely confidentiality, authentication, integrity, and anti-denial (Menezes *et al.*, 1996).

1. Confidentiality

   Confidentiality service is a security service that safeguards information from parties who are not entitled to have it. An encryption process can guarantee this service.

2. Authentication

   Authentication is a security service that ensures that the parties involved in the communication process are identified parties. This authentication service is divided into two mechanisms, namely entity authentication, and data origin authentication. Entity authentication provides guarantees to the parties involved in the communication process, whereas authentication of data origin provides assurance of the validity of data sources.

3. Integrity

   Integrity is a security service that guarantees the authenticity of some information. With this service, the recipient can be sure that the information received has not been changed or manipulated during the transmission process.

4. Anti disclaimer

   An anti-denial service is a security service that ensures the sender cannot deny the messages it has sent.

2.4 Rivest-Shamir-Adleman (RSA)

Of the many public-key cryptographic algorithms that have been made, the most popular algorithm is the RSA algorithm (Ariyus, 2015). This algorithm performs factoring of large numbers. For these reasons, RSA is considered safe. To generate two chords, two large random prime numbers are selected. Three researchers developed the RSA algorithm from the Massachusetts Institute of Technology (MIT) in 1976, namely Ron Rivest, Adi Shamir, and Leonard Adleman.

RSA express the original text, which is encrypted into blocks where each block has a binary number value which is given the symbol "n", the original text block "M" and the text block code "C". To encrypt the message "M", the message is divided into numeric blocks smaller than "n" (binary data with the largest power) if the prime number is 200 digits long, a few bits of 0 to the left of the number can be added to keep the message remains less than the value "n".

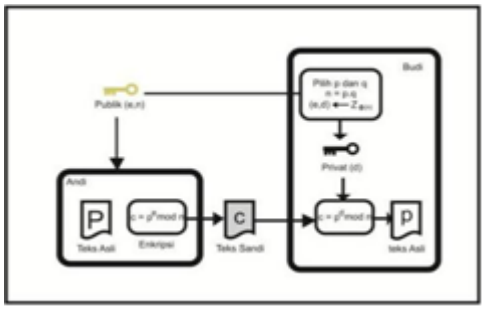

Figure 1. RSA system

2.4.1 RSA Key Generation

The decryption (Budi) generates a pair of keys to use RSA, namely the public key and the private key (Sadikin, 2015). The first thing the key generator algorithm does is generate two large prime numbers. The generation of large prime numbers uses prime number testing algorithms such as the Miller-Rabin algorithm. Following are the steps for generating the RSA key:

1. Generate prime numbers of p and q

$$N = p * q \quad (1)$$

$$Ø(n) = (p - 1) * (q - 1) \quad (2)$$

$$e \overset{r}{\leftarrow} Z_{Ø(n)} \text{ with gcd } (e, Ø_{(n)}) = 1 \quad (3)$$

$$d = e^{-1} \text{ in } Z_{Ø(n)} \quad (4)$$

$$K_{public} = (e, n), K_{private} = d \quad (5)$$

In order for the RSA cryptography system to be secure, large prime numbers are needed so that n = p x q is very difficult to factorize. The recommended size of p and q is 512 bits so that n is 1024 bits.

2.4.2 RSA Encryption Process

After the public key K_{public} generated by the decryption (Budi), anyone can use the public key to send a coded text message to Budi. The RSA encryption algorithm uses an exponential function in modular n (Sadikin, 2015). Here are the RSA encryption steps:

1. Input: $K_{public} = (e, n)$, $P \in Z_n$
2. Output: $C \in Z_n$

$$C = P^e \text{mod } n \text{ (Use the Square and Multiply algorithms)} \quad (6)$$

2.4.3 RSA Decryption Process

If Budi gets the ciphertext that is encrypted with Budi's public key, Budi can use his private key to return the ciphertext to the original text (Sadikin, 2015). The following is the formula for the description of the RSA:

1. Input: $K_{private} = d$, $K_{public} = (e, n)$, $C \in Z_n$
2. Output: $P \in Z_n$

$$P = C^d \bmod n \tag{7}$$

2.4.4 RSA Cryptographic Evidence System

The RSA description function can be proven which is the inverse (inverse) of the RSA encryption function, by using the Euler theorem (Sadikin, 2015). The parameter relationship d in the private key and e in the public key can be written as follows:

$$e.d \equiv 1 \bmod Ø(n)$$

Therefore, with modular arithmetic, it can be written as:

$$e.d \equiv tØ(n + 1)$$

With an integer $t \geq 1$. Function RSA encryption restores $C = P^e \bmod n$, so the RSA description can be calculated as:

$$\begin{aligned} P &= C^d \bmod n \\ &= P^{e.d} \bmod n \\ &= P^{tØ(n)+1} \bmod n \\ &= P^{tØ(n)}.P \bmod n \\ &= 1^t.P \bmod n \text{ with Euler's Theorem} \\ &= P \bmod n \end{aligned}$$

Therefore, the RSA description algorithm is an inverse of RSA encryption.

2.5 AES (Advanced Encryption Standard)

AES is a non-Feistel block encoding system because this algorithm uses inverse components with a block length of 128 bits (Sadikin, 2015). AES keys can be 128, 192, and 256 bits in length. AES encryption uses an iterative process known as a round. The number of rounds depends on the length of the chord used. Each round requires a round key and input from the next round. Round keys are generated based on the given key. The relationship between the number of rounds and the length of the chord is as follows:

AES Key Length (bits)	Number of Round (Nr)
128	10
192	12
256	14

Table 1. Number of rounds and key length (Sadikin, 2015) AES key

2.5.1 AES Encryption Process

The AES encryption process is a state transformation. A text in blocks (128 bits) will first be organized as a state. AES encryption is a state transformation that is repeated over several rounds (Sadikin, 2015).

Initially, the original text will be reorganized as a state. Before round 1 starts the original block of text mixed with the key to round 0 of this transformation called AddRoundKey. After that, round 1 to round (Nr-1) where Nr is the number of rounds using 4 types of transformations, namely sub

bytes, shiftrows, mixcoloumns, and add round key. In the last round, the Nr round was carried out the transformation is similar to the other rounds but without the mixcoloumns transformation.

2.5.2 Decryption Process AES

In summary, the AES decryption algorithm is the opposite of the AES encryption algorithm. The AES description uses the basic transformations used in the AES encryption algorithm. Each AES basic transformation has an inverse transformation, namely inv sub by test, inv shift rows, and inv mix columns (Sadikin, 2015).

2.6 Digital Signature

The security aspects that are generally provided by cryptography are as follows.

1. Confidentiality / secrecy
2. Authentication (authentication)
3. The authenticity of the message (data integrity).
4. Anti-denial (nonrepudiation).

Aspect one is solved by encryption/decryption. While aspects 2 to 4 are solved with a digital signature.

The signature has the following characteristics:

1. The signature is authentic evidence.
2. The signature cannot be forgotten.
3. The signature cannot be moved for reuse.
4. Signed documents cannot be changed.
5. The signature cannot be denied (repudiation).

The signature function on paper documents is also implemented for authentication on digital data (messages, electronic documents). Signatures for digital data are called digital signature. The digital signature is not a digitized (scanned) signature; however, a digital signature is a cryptographic value that depends on the message content and key.

The signature on a printed document is always the same, regardless of the content of the document. Digital signatures always vary from document content to document. One way that you can use to sign messages with a digital signature is by using combination function hash (hash function) and public-key cryptography.

In general, signing a message in a way that encrypts always gives two functions: message confidentiality and message authentication. However, in some cases, authentication is often required, but the message's confidentiality is not. This authenticity is described as follows:

1. If the received M (Message) message has changed, the MD's message digest generated from the hash function is different from the original MD message digest. This means the message is no longer original.
2. If the message M does not come from an actual person, then the MD generated from equation 3 is different from the MD' generated in the verification process (this is because the public key used by the message recipient does not correspond to the sender's private key).
3. If MD = MD', this means the message received is message authentication, and the person who sent it is the real person (user authentication).

2.7 Related Research

No.	Researcher	Title	Methodology	Result
1.	1. Alamsyah 2. Agus Bejo 3. Teguh Bharata Adji	The replacement of irreducible polynomial and affine mapping for the instruction of a strong S-box	Replacement of Polynomial and Affine	The proposed S-box has a level of security that is more than the existence of other S-box.
2.	1. Pon. Partheeban 2. V. Kavitha	Dynamic key dependent AES S-box generation with optimized quality analysis.	Designing dynamic S-box that is high non-linearity and low autocorrelation.	S-box designed ultimately as high non-linearity and low autocorrelation.
3.	1. Carmit Hazay 2. Gert Laessoe Mikkelsen 3. Tal Rabin 4. Tomas Toft 5. Angelo Agatino Nicolosi	Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting.	Composite RSA as part of a CRS for secure computing on files.	Paillier decryption to perform to do Paillier decryption with the new threshold key. The party file must increase the ciphertext with an extension of the protocol presented for the two-party case.
4.	1. Orr Dunkelman 2. Nathan Keller 3. Adi Shamir	Improved Single-Key Attack on 8-Round AES-192 and AES-256.	AES-192 and AES-256 algorithm.	The introduction of the new cryptalization technique that can be used to increase complexity in rounds 7 and 8 of AES.

3 Method

The method used in previous research is algorithm RivestCode5 (RC5) (Suryawan & Hamdani, 2013), RSA (Erika, Rachmawati, & Surya, 2012), and AES (Pabokory, Astuti, & Kridalaksana, 2015).

3.1 Data Source

3.1.1 Primary Data

Primary data in this study were obtained by means of interviews. The obtained data are in the form of website data and solutions to protect data.

3.1.2 Secondary Data

Secondary data in this study were obtained through literature review.

3.2 Literature Review

A literature study is carried out by collecting data and information obtained by reading and studying books, research journals, international seminars, and others related to this research.

3.3 RSA and AES Algorithm Encryption Flowchart

Making a flowchart on encryption will be used to explain the flow of the encryption system on data security using the RSA and AES algorithms.

3.4 Flowchart Description of RSA and AES Algorithms

The making of this flowchart will explain how the decryption system flows on messages that have been encrypted or in the form of ciphertext, and the decryption process uses the AES and RSA algorithms.

4 Results

The development tools used in the related research of comparative cryptographic performance RSA and AES was NetBeans IDEA 12.0. Figure 2 illustrates an overview of the system used in the related study.

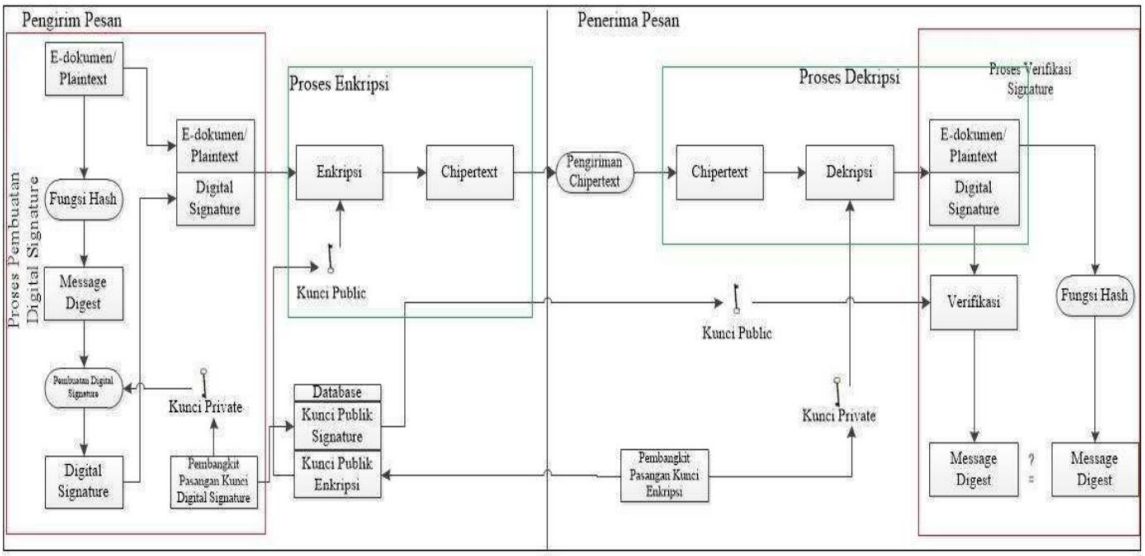

Figure 2. Digital signature workflow

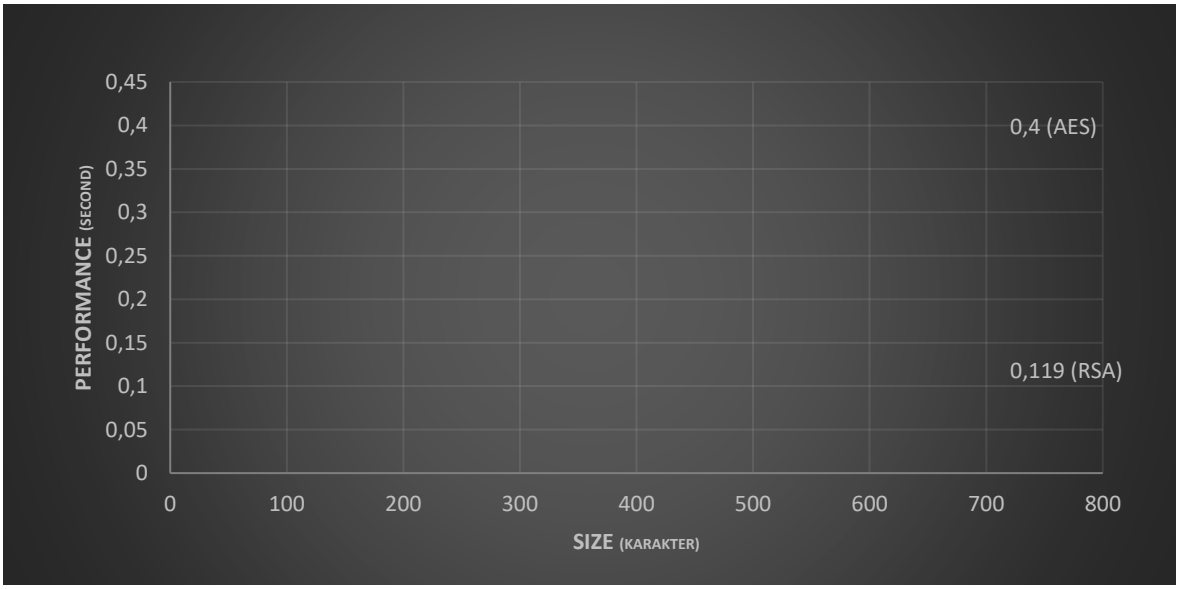

Figure 3. RSA and AES performance

Figure 3 shows the AES encryption and decryption process takes quite some time (0,4 seconds) compared to RSA (0,1 seconds). The comparison of the stability of each algorithm can be seen in Figure 4.

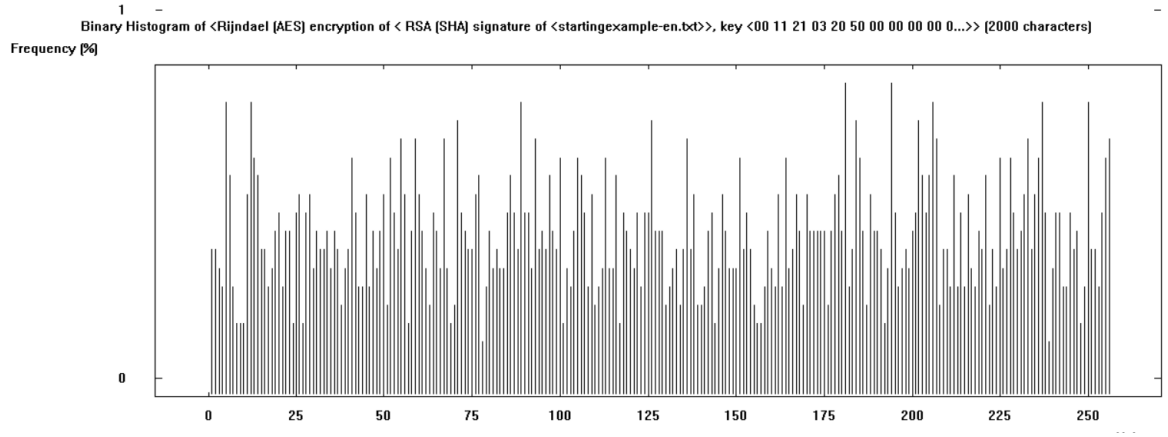

Figure 4. Binary histogram of AES encryption

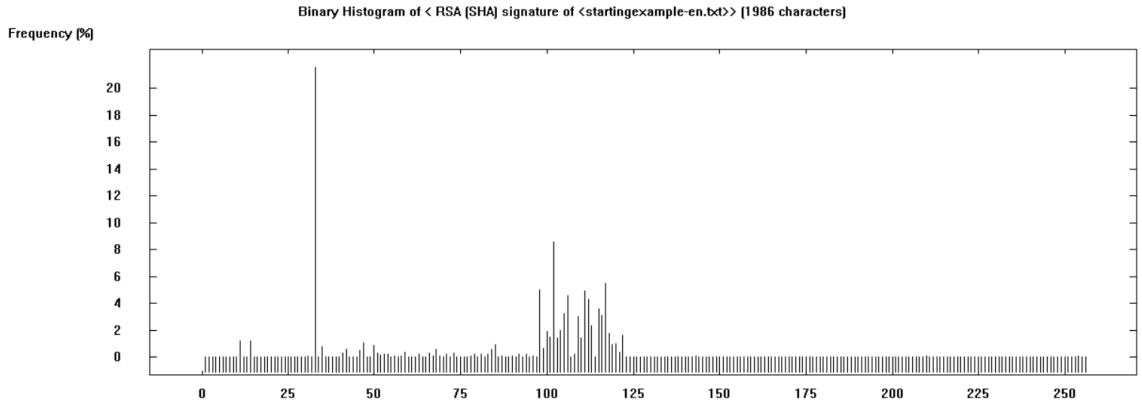

Figure 5. Binary histogram of RSA (SHA)

Figure 5 depicts the AES histogram is very unstable when compared to the RSA histogram.

5 Conclusion

From the research method used, conclusions were drawn; what is obtained in this study is about how the performance of the results using libraries and existing data that RSA has a more stable performance compared to AES.

References

Alamsyah, Bejo, A., Adji, T. B. (2017). AES S-box Construction using Different Irreducible Polynomial and Constant 8-bit Vector. In *2017 IEEE Conference on Dependable and Secure Computing*, 366–369. doi:10.1109/DESEC.2017.8073857

Alyanto, D. (2016). Penerapan Algoritma AES: *Rijndael dalam Pengenkripsian Data Rahasia [Application of AES Algorithm: Rijndael in Encrypting Confidential Data]* (Bachelor's Thesis). Retrieved from https://docplayer.info/36742114-Penerapan-algoritma-aes-rijndael-dalam-pengenkripsian-data-rahasia.html

Anwar, N., Munawwar, M., Abduh, M., & Santosa, N. B. (2018, December). Komparatif Performance Model Keamanan menggunakan Metode Algoritma AES 256 Bit dan RSA [Model Performance Security Comparative using AES 256 Bit Algorithm Method and RSA]. *Jurnal Rekayasa Sistem dan Teknologi Informasi (RESTI),* 2(3), 783-791. Retrieved from http://jurnal.iaii.or.id/index.php/RESTI/article/view/606

Aufa, F. J., Endroyono, E., Affandi, A. (2018). Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm. In *Conference: 2018 4th International Conference on Science and Technology (ICST)*, 1-5. doi:10.1109/ICSTC.2018.8528584

Belazi, A., Khan, M., El-Latif, A. A. A, Belghith, S. (2017). Efficient Cryptosystem Approaches: S-boxes and Permutation–Substitution-based Encryption. *Nonlinear Dynamics*. 87, 337-361. doi:10.1007/s11071-016-3046-0

Delfs, H., & Knebl, H. (2015). *Introduction to Cryptography: Principles and Applications, Symmetric-key Encryption* (3rd Ed.). Manhattan, NYC: Springer Publishing.

Farah, T., Rhouma, R., & Belghith, S. (2017). A Novel Method for Designing S-box Based on Chaotic Map and Teaching - Learning-Based Optimization. *Nonlinear Dynamics*, 88(2), 1059–1074. doi:10.1007/s11071-016-3295-y

Isa, H., Jamil, N., & Aba, M. R. Z. (2016). Construction of Cryptographically Strong S-boxes Inspired by Bee Waggle Dance. *New Generation Computing*, 34, 221–238. doi:10.1007/s00354-016-0302-2

Lambić, D. (2017). A Novel Method of S-box Design Based on Discrete Chaotic Folder. *Nonlinear Dyn*amics, 87(4), 2407–2413. doi:10.1007/s11071-016-3199-x

Liu, J., Mesnager, S., & Chen, L. (2017). On the Nonlinearity of S-boxes and Linear Codes. *Cryptography and Communication*, 9(3), 345–361. doi:10.1007/s12095-015-0176-z

Pabokory, F. N, Astuti, I. F, & Kridalaksana, A. H. (2015). Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen menggunakan Algoritma Advanced Encryption Standard [Cryptography Data Security Implementation in Text Messages, Document File Contents, and Document Files using the Advanced Encryption Standard Algorithm]. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, 10(1), 20-31. doi:10.30872/jim.v10i1.23

Partheeban, P., Kavitha, V. (2018) Dynamic Key Dependent AES S-box Generation with Optimized Quality Analysis. *Cluster Computing*, 22, 14731-14741. doi:10.1007/s10586-018-2386-6

Sadikin, M. A., & Wardhani, R. W. (2016, July). Implementation of RSA 2048-bit and AES 256-bit with Digital Signature for Secure Electronic Health Record Application. In *International Seminar on Intelligent Technology and Its Applications (ISITIA)*. IEEE. doi:10.1109/ISITIA.2016.7828691

Stalling, W. (1999). Cryptography and Network Security: Principles and Practice (2nd Ed.). Upper Saddle River, NJ: Prentice-Hall, Inc.

Utama, K. D. B., Al-Ghazali, Q. M. R., Mahendra, L. I. B., & Shidik, G. F. (2017, October). Digital Signature using MAC Address based AES-128 and SHA-2 256-bit. In *2017 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 72-78. IEEE. doi:10.1109/ISEMANTIC.2017.8251846

Wanda, P. (2016). Efisiensi Pengamanan Pesan Mobile Banking Berbasis Algoritma Advanced Encryption Standard (AES) [Mobile Banking Message Security Efficiency Based on the Advanced Encryption Standard (AES) Algorithm]. *Seminar Nasional Teknologi dan Multimedia (Semnasteknomedia)*, 4(1), 13-20. Retrieved from https://ojs.amikom.ac.id/index.php/semnasteknomedia/article/view/1142/1098

Widarma, A. (2016). Combination AES, RC4 and ElGamal Algorithms in Hybrid Scheme for Data Security. *Computer Engineering, Science and System Journal*, 1, 1-8. doi:10.24114/cess.v1i1.4040

Xu, T., Liu, F., Wu, C. (2017). A White-box AES-like Implementation Based on Key-dependent Substitution-linear Transformations. *Multimedia Tools and Application*, 77, 18117–18137. doi:10.1007/s11042-017-4562-8