Taris Monica

by fofoi id

Submission date: 22-Aug-2024 09:23AM (UTC+0700)
Submission ID: 2435853272
File name: 8654-23484-1-RV.docx (523.85K)
Word count: 3542
Character count: 19119

JIKO (Jurnal Informatika dan Komputer)
Vol. x, No. x, April 2024, pp. x-x
DOI: 10.33387/jiko

Accredited KEMENDIKBUD RISTEK, No.105/E/KPT/2022
p-ISSN: 2614-8897
e-ISSN: 2656-1948

QUESTION BANK SECURITY USING RIVEST SHAMIR ADLEMAN ALGORITHM AND ADVANCED ENCRYPTION STANDARD

Taris Monica[1], Asep Id Hadiana[2], Melina[3]

[1,2,3]Department of Informatics, Faculty of Science and Informatics, Universitas Jenderal Achmad Yani, Cimahi, Indonesia

*Email: [1] tarismonica@if.unjani.ac.id, [2]asep.hadiana@lecture.unjani.ac.id, [3]melina@lecture.unjani.ac.id

(Received: dd mmm yyyy, Revised: dd mmm yyyy, Accepted: dd mmm yyyy)

Abstract

Data security is important. Educational question banks at Vocational High Schools (SMK) contain confidential information that could potentially be misused if not properly secured. This research aims to secure student question bank data and develop a responsive web platform at Pusdikhubad Cimahi Vocational School by implementing the integration of the Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) cryptographic algorithms through the encryption and decryption process. AES is a symmetric key cryptography algorithm and RSA is an encryption algorithm based on the use of public keys to encrypt the keys required by AES-256. The integration of these two algorithms aims to ensure data confidentiality, prevent manipulation, and facilitate access to exam materials by authorized parties. The results of this research show that the process of encrypting and decrypting question data using a combination of RSA and AES was successfully carried out on the question bank system. Avalanche Effect testing shows that RSA and AES 256 bit encryption have an Avalanche Effect level of 49,99% %. Apart from that, the results of the system feasibility test using a black box show that the SIFILE system has a percentage level of 100%. It is hoped that the results of this research can become a data security system at Pusdikhubad Cimahi Vocational School and other educational institutions in securing the question bank from unauthorized access.

Keywords: *RSA algorithm, AES-256, Question bank, Data security, Cryptography.*

**Corresponding Author*: *Taris Monica*

1. INTRODUCTION

The rapid advancement of technology, particularly in information exchange, enables swift access and exchange of data. However, this progress also amplifies the risk of cybercrimes, such as hacking activities conducted by individuals or groups who illegally acquire sensitive information. The development of technology has also influenced the educational environment by enhancing quality, speed, practicality, and convenience. In educational settings, question banks stored in databases are crucial assets that need to be protected [1]. To prevent unauthorized access by hackers or other unauthorized parties, data security becomes a critical aspect [2]. Protecting exam data on computers that lack special security measures requires effective methods to ensure confidentiality and prevent misuse [3].

Sekolah Menengah Kejuruan (SMK) Pusdikhubad Cimahi, a private vocational high school located at Jl. Kalidam No.1, Cimahi Tengah, Kota Cimahi, was first inaugurated in 1974. Initially known as STM Elektronika, SMK Pusdikhubad was established by the Pusat Pendidikan Perhubungan (PUSDIKHUB TNI-AD). All teaching and learning activities are centered at PUSDIKHUB TNI-AD. In 1994, the school was renamed SMK Pusdikhubad and began implementing the Electronic Communication Engineering Expertise Program using the 1994 curriculum. Pudikhubad Cimahi faces challenges in protecting its question banks from increasing security risks, including potential data leaks and illegal access, which could threaten academic integrity and educational fairness [4].

Currently, SMK Pusdikhubad Cimahi still uses manual methods, such as physical (hardcopy) formats, to manage its question banks. This method presents several problems, including the vulnerability of hardcopy stored questions to leakage, whether through internal or external misuse. To address these issues, a

concept of data access was developed by securing document files. In this concept, when a question bank is uploaded, the data will be encrypted first. To encrypt the document, the user must also enter a secret key provided by the system, allowing the data to be automatically encrypted. To maintain data security, prevent hijacking, and avoid misuse of information, this system ensures the confidentiality of the question bank. An effective method is required to safeguard data privacy, keep it secure, and protect it from misuse [5].

One of the ways to ensure the security and confidentiality of data within a system is by using cryptographic algorithms. These algorithms use mathematical concepts such as algorithms, encryption keys, and hash functions to protect data from threats [6]. The Advanced Encryption Standard (AES) is a highly secure cryptographic algorithm used as an encryption standard for sensitive information and is widely adopted worldwide. AES generates symmetrically encrypted data, while the Rivest Shamir Adleman (RSA) algorithm encrypts data using a public key and decrypts it with a private key. RSA is a type of public-key cryptography, also known as asymmetric cryptography, where each user has a pair of cryptographic keys: a public key and a private key [7].

RSA is an encryption algorithm based on the use of a public key, a key aspect of cryptography, which plays a role in the encryption process and digital signature creation. RSA has become a common standard in Electronic Commerce protocols and is trusted as a secure method for safeguarding data using sufficiently large key lengths [8]. On the other hand, AES is an encryption block cipher issued by the National Institute of Standards and Technology (NIST) in 2000. RSA and AES are key to data security in various sectors, including finance, where RSA provides secure key exchange, and AES offers efficient data encryption [9]. These two algorithms are chosen for their ability to provide reliable security while maintaining operational efficiency.

Several studies have examined data security using RSA and AES algorithms [10], such as the study which applied AES cryptography-based QR Code in medical record administration, focusing on data security, particularly the confidentiality of patient, doctor, and healthcare facility information. This study aimed to address data security challenges by integrating AES and QR Code. Testing was conducted using a default password (admin) and a specific key, resulting in cipher transformation from the password. The testing process enabled decryption of the cipher and key, demonstrating that the use of the AES method is an effective solution for enhancing data security in medical record administration for the future. Another study [11] on the verification method of Electronic Signatures (TTE) using KKPS-based authentication techniques with the RSA algorithm was proven effective in ensuring the authenticity and integrity of related electronic information. The research result showed that the use of the RSA algorithm in KKPS is a strong method for ensuring the integrity, authentication, and security of information in TTE. Furthermore [12], research discusses the development and implementation of a cryptography application that uses a combination of two algorithms, RSA and AES, to enhance data security. The RSA algorithm is used to generate public and private keys and to encrypt secret keys, while the AES algorithm is used to encrypt plaintext. This system is designed to ensure that messages sent are more secure, as they must undergo double encryption and decryption processes involving both algorithms.

Based on previous research, numerous studies have examined RSA and AES algorithms, but there is still a lack of research focusing on the security of question banks by combining RSA and AES algorithms on a responsive website platform. Therefore, this study combines RSA and AES algorithms to enhance the security of question banks. The results of this research are expected to improve the security of exam documents in the context of website-based services.

2. RESEARCH METHOD

This research method describes the design of the question bank file storage system for teachers and software design, to the user interface of the software built.

2.1 Research Stages

This research method involves several important stages as shown in the figure. The first stage is the generation of the private key and public key through the RSA Key Generation process. The generated public key is used to encrypt the secret key using the RSA Encrypt algorithm. The encrypted secret key is then used to encrypt the plaintext into ciphertext using the AES Encrypt algorithm.

After the encryption process is complete, the ciphertext and secret key encrypted payload are sent to the recipient. The receiver then decrypts the secret key encrypted payload using the private key through the RSA Decrypt process to get the original secret key. This secret key is used to decrypt the ciphertext using the AES Decrypt algorithm, resulting in the original plaintext.

This process ensures security in data exchange between the sender and receiver through layered encryption, with a combination of RSA and AES methods, as shown in methods study in figure 1.

Figure 1. Research method

2.2 Software Design

This process ensures that all aspects of the software meet the specifications and user needs, thereby reducing errors and increasing development efficiency. The first step is to classify software requirements into two main categories, namely Non-Functional and Functional requirements. Next is the use case diagram which provides an overview of the system's behavior when responding to user requests which is then described to provide an explanation of the response by the system called the use case scenario. Next is the activity diagram which is used by user actors to describe the classification data managed by the system, then the sequence diagram which will show the interactions around the system and the interactions between objects and will produce certain outputs, then the class diagram which provides an overview of the system structure based on the definition of the desired class formed in the creation of a system and the last step is to design an interface framework that aims to design the interface used and the results in accordance with user needs.

3. CRYPTOGRAPHY

Cryptography is like the art of hiding messages, where the original text (plaintext) is converted into random code (ciphertext) using special keys and algorithms. Without the right key, ciphertext is like a sea of unreadable words [13].

3.1 Rivest Sharim Adleman (RSA)

RSA is an encryption algorithm based on the use of public keys. is recognised as one of the most important in public key cryptography, used for both encryption and digital signatures. RSA has become a common standard in electronic commerce protocols and is believed to be a secure method for securing data using keys that have a large enough length [14]. In the RSA algorithm there are 3 stages or processes that are usually carried out, namely key generation, encryption and decryption [5].

Key Generation

The RSA algorithm requires 2 keys, a public key and a private key. The steps for key generation are:

Key Generator

1. Choose two prime numbers that are large enough, namely p and q. The values of p and q must be kept secret.
2. Calculate the modulus (n) as the product of p and q using the equation (1).
$$n = p \times q \quad (1)$$
3. Calculate the Euler Totien function (φ(n)) as the product of $(p-1)$ and $(q-1)$ using the equation (2).
$$\varphi(n) = (p-1) \times (q-1) \quad (2)$$
4. Choose an integer e (usually prime relative to $\varphi(n)$ and less than $\varphi(n)$) as the public key, using equation (3).
$$e = \frac{1+\varphi(n)}{d} \quad (3)$$
where
$i: 1, 2, 3, 4, \ldots . n$
d : prime number $<$ $\varphi(n)$
e : public key
5. Calculate the integer d for the private key with the equation (4).
$$(d \times e)\ mod\ \varphi(n) = 1 \quad (4)$$
where
d: private key.

Encryption Process

In the encryption process, the plaintext (P) is converted into an integer corresponding to the message using a mapping scheme, and usually using an ASCII or Unicode table. The encryption process into ciphertext (C) is carried out using the equation (5).
$$C = (P^e)\ mod\ n \quad (5)$$

Decryption Process

The decryption process to return the ciphertext to plaintext is carried out again using equation (6)
$$P = (C^d)\ mod\ n \quad (6)$$
where
P : *plaintext*
C : *ciphertext*
d : private key
n : the result of multiplying prime numbers.

3.2 Advanced Standard Encryption (AES)

The Advanced Standard Encryption Algorithm (AES) is a type of block encryption algorithm created and published by the National Institute of Standards and Technology (NIST) in 2000. This algorithm works by encrypting data into small secure blocks [15]. AES 128 bit is like a secret key that works both ways, locking and unlocking messages with the same key.

Compared to longer AES keys, AES 128 bit works faster and more compact, using fewer rounds to secure your data [16].

The AES algorithm uses round cycles in its encryption process. Each round is affected by the key length which is divided into 10, 12, or 14 rounds depending on the key length used. The AES encryption process includes SubBytes, ShiftRows, MixColumns, and AddRoundKey. The AddRoundKey process is first applied, followed by SubBytes, ShiftRows, MixColumns, and AddRoundKey, and this cycle is repeated for the specified number of rounds. AES is shown in the table 1.

Table 1. AES

Algorithm	Key Length (bits)	Block Size (bits)	No of Round
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

3.3 Authentication

Authentication is a user validation process when entering a system. Authentication aims to verify the user's identity validly [17].

3.4 Encryption Process

The encryption process involves four types of byte transformations in the AES algorithm. First, AddRoundKey uses an XOR operation between plaintext and cipher key. Then, SubBytes replaces the bytes in the state with values from the substitution table (S-Box). ShiftRows involves shifting bytes on each row in the state array, while MixColumns involves shuffling the data in each column of the state array [16].

In the initial stage of encryption, the state is changed using AddRoundKey. Then, the state undergoes the transformation of SubBytes, ShiftRows, and MixColumns repeatedly Nr, which is called the Round Function. In the last round, the state does not undergo MixColumns transformation. Figure 2.2 shows the steps in the AES algorithm encryption process [15].

4. RESULT AND DISCUSSION

The results of software quality and testing involve assessing the accuracy of the developed machine learning model.

4. 1 Implementation System

At this stage, the focus is on the implementation of the software in accordance with the design previously described in Chapter III. Implementation is done locally using a personal computer to facilitate testing. The software developed is web-based using PHP as the main programming language, Visual Studio Code as a development tool, Google Chrome as a web browser, as well as MySQL as a database and Apache from XAMPP as a web server.

4. 2 Interface Implementation

The form of implementation of the system interface that is built is a website that displays the application home page and encryption page as well as an explanation of the question document that displays the results of the avalanche effect test in size (bytes) before encryption and after encryption that have been previously entered on the website. Successively shown in the following figure:

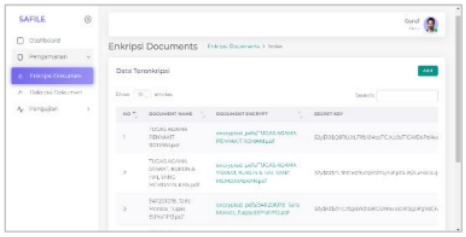

Figure 2. Encryption Page

Figure 3. Add Question Document Page

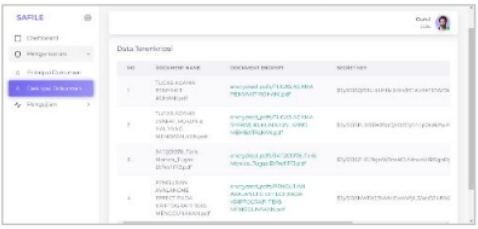

Figure 4. Description Page

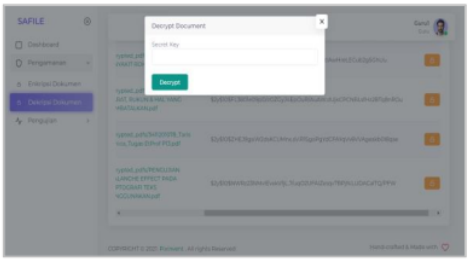

Figure 5. Secret Key Description Form Page

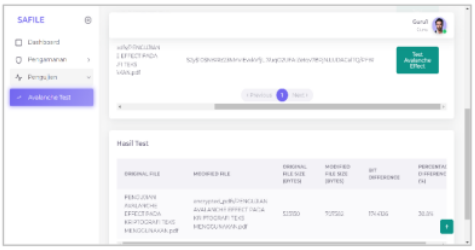

Figure 6. Avalanche Effect Testing Form Page

4. 3 Testing Software

The results of blackbox testing on the design of the 'SIFILE Application' show that all features are in accordance with the design that has been made. All test cases in the system can run as expected. The percentage of conformity is calculated based on the test results as follows:

1. Number of test codes: 4 test codes
2. Corresponding result test code: 4 test codes
3. Unsuitable result test code: 0 test code

Based on the test results conducted on the decision support system can be seen in the calculation of the percentage of the system against the calculation data with the following equation (7).

$$\text{Result} = \frac{(\text{number of unsuitable test codes})}{\text{number of test codes}} \times 100\% \qquad (7)$$

$$= \frac{(4-0)}{4} \times 100\% = 100\%$$

The results of the system suitability evaluation show that software testing using the blackbox testing method has met all the specifications set with 100% accuracy.

4. 4 System Testing

Testing is an activity to evaluate a system that has been developed to ensure compliance with the design that has been determined. This research uses Black Box Testing to test software functionality, focusing on this aspect.

Table 1. Blackbox testing

No	Test Code	Expected Response	Result
1	KU-001) Perform the process of adding question documents	The system can display documents from question documents	in accordance
2	(KU-002) Encrypt the question document and secret key	The system can encrypt the question document and the inputted secret key	in accordance
3	(KU-003) Decrypt the secret key and question document	The system can encrypt the secret key and the inputted question document.	in accordance
4	(KU-004) Conduct avalanche effect testing	The system can calculate and display avalanche effect test results	in accordance

4. 5 Avalanche Effect Test Result

Avalanche Effect (AE) testing is carried out by analyzing changes in bit values from the encryption results in the system. The following is an example of the experiment carried out which is shown in Figure 7,8,and 9.

1. Experiment 1 (Change the first 1 character)
   a. Plainteks
      Plainteks : smk pusdik hubad
      Key : SMKHUBADCimahiSMKHUBAD
      Kriptografi : RSA, AES 256-bit
   b. Chiper Text
      Before ffvC7zSAPpLY6I9yixXvkqAGXXVAVyihBLaJPaCqWPc=
      After 5ONguymxUxzHxxqvjhsqB6leOVWX4r/N313ddTheH0Y=
   c. Conversion in Bit :
      Before 01111101 11111011 11000010 11101111 00110100 10000000 00111110 10010010 11011000 11101000 10001111 01110010 10001011 00010101 11101111 10010010 10100000 00000110 01011101 01110101 01000000 01010111 00101000 10100001 00000100 10110110 10001001 00111101 10100000 10101010 01011000 11110111
      After 11100100 11100011 01100000 10111011 00101001 10110001 01010011 00011100 11000111 11000111 00011010 10101111 10001110 00011011 00101010 00000111 10101001 01011110 00111001 01010101 10010111 11100010 10111111 11001101 11011111 01011101 11011101 01110101 00111000 01011110 00011111 01000110
   d. Calculation Avalanche Effect

$$Avalanche\ Effect = \frac{123}{256} \times 100\% = 48{,}04\%$$

Figure 7. Example 1 Avalanche Effect Testing

2. Experiment 2 (Change 1 middle character)
   Before smk pusdik hubad
   After smk ausdik hubad
   a. Chiper Text
   Before ffvC7zSAPpLY6I9yixXvkqAGXXVAVyihBLaJPaCqWPc=
   After TWnhY6x/+pSeLObqBWEmqD1FqNyIwSe6zdd2Xlfc4Mo=
   b. Conversion ini Bit :
   Before 01111101 11111011 11000010 11101111 00110100 10000000 00111110 10010010 11011000 11101000 10001111 01110010 10001011 00010101 11101111 10010010 10100000 00000110 01011101 01110101 01000000 01010111 00101000 10100001 00000100 10110110 10001001 00111101 10100000 10101010 01011000 11110111
   After 01001101 01101001 11100001 01100011 10101100 01111111 11111010 10010100 10011110 00101100 11100110 11101010 00000101 01100001 00100110 10101000 00111101 01000101 10101000 11011100 10100101 11000001 00100111 10111010 11001101 11010111 01110110 01011110 01010111 11011100 11100000 11001010
   c. Calculation Avalanche Effect

$$Avalanche\ Effect = \frac{131}{256} \times 100\% = 51{,}17\%$$

Figure 8. Example 2 Avalanche Effect Testing

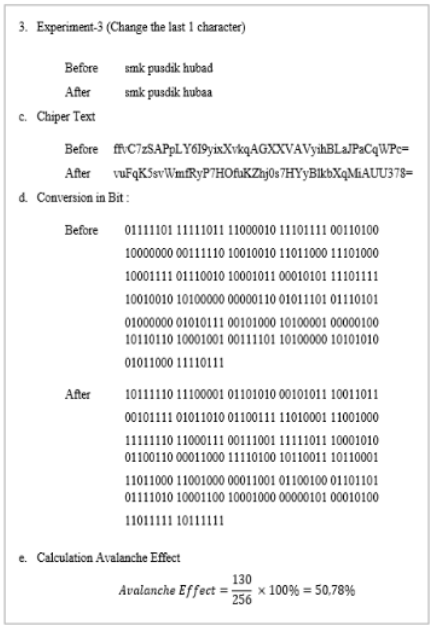

Figure 9. Example 3 Avalanche Effect Testing

Table 2. Avalanche effect result

No	Secret Key	Document Encrypted	Bit Difference	Value Avalanche
1	Taris19	707582	1744126	30.8%
2	TarisMonica19	464882	1140035	30.7%
3	Encrypted2024	123316	293044	29.7%
4	Enkripsi$123	707582	1744126	30.8%
5	UTS@P12	271010	659135	30.4%
			Average	30.48%

Based on the 3 experiments that have been carried out, the Avalanche Effect (AE) value obtained in the 1st experiment was 48.04%, in the 2nd experiment it was 51.17% and in the 3rd experiment it was 50.78%. If calculated, the average value obtained is 49.99%. Based on the average calculation, it can be concluded that the AE test value is adequate because it is in the range of 45% - 60%.

4. 6 Implementation of Avalanche Effect

Based on the avalanche effect test results, there is a question document that was tested with the overall average obtained for the avalanche effect result of 30.48% which indicates that the AES cryptographic algorithm on the question document has a good avalanche effect value because large changes in plaintext can have an impact on ciphertext because there are several bits that change. But from the test results above, the use of a more complicated secret key (such as the use of spaces, numbers, and characters) does not affect the encryption results of the question document when viewed based on the resulting avalanche effect value.

5. CONCLUSION

The test results show that the combination of RSA and AES algorithms provides a good security layer. Avalanche effect testing shows that RSA and AES 256 bit encryption has an Avalanche Effect rate of 30.48%. In addition, the results of the system feasibility test using blackbox show that the SIFILE system has a percentage level of 100% and is feasible to use.

REFERENCES

[1] I. Solikhin, M. Sobri, and R. Saputra, "Sistem Informasi Pendataan Pengunjung Perpustakaan," *J. Ilm. Betrik*, vol. 9, no. 03, pp. 140–151, 2018.

[2] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "A Good Performance OTP encryption image based on DCT-DWT steganography," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 15, no. 4, pp. 1987–1995, Dec. 2017, doi: 10.12928/TELKOMNIKA.v15i4.5883.

[3] M. Safii, "KRIPTOGRAFI MONOALFABETIK DAN POLIALFABETIK APLIKASI DAN KOMPARASI DALAM PENGAMANAN DATABASE BANK SOAL".

[4] "Profil SMK Pusdikhubad, Kota Cimahi (PPDB, Biaya Masuk, Pendaftaran) - Sekolahloka."

[5] F. Farhan and D. Leman, "Implementasi Metode Rivest Shamir Adleman (RSA) Untuk Kerahasiaan Database Perum Bulog Kanwil SUMUT," *J. Mach. Learn. Data Anal.*, vol. 02, no. 01, pp. 18–27.

[6] A. Triono, A. S. Budi, R. Abdillah, and V. Cipher, "Implementasi peretasan sandi vigenere chipher menggunakan bahasa pemrograman python," vol. 1, no. 1, pp. 1–9, 2023.

[7] "UNES Journal of Information System COMPARISON OF SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHIC," vol. 8, no. 1, pp. 42–47, 2023.

[8] J. Hutagalung, P. S. Ramadhan, S. J. Sihombing, and P. Korespondensi, "KEAMANAN DATA MENGGUNAKAN SECURE HASHING ALGORITHM (SHA) - 256 DAN RIVEST SHAMIR ADLEMAN (RSA) PADA DIGITAL SIGNATURE IMPLEMENTATION OF SECURE HASHING ALGORITHM (SHA) -256 AND RIVEST SHAMIR ADLEMAN (RSA) ON DIGITAL SIGNATURE," vol. 10, no.

6, 2023, doi: 10.25126/jtiik.2023107319.
[9] A. N. Agustina, "PENGAMANAN DOKUMEN MENGGUNAKAN METODE RSA (RIVEST SHAMIR ADLEMAN) BERBASIS WEB," pp. 14–19, 2015.
[10] A. Id Hadiana, F. Rakhmat Umbara, J. Terusan Jend Sudirman, K. Cimahi Sel, K. Cimahi, and J. Barat, "PENGGUNAAN QR CODE BERBASIS KRIPTOGRAFI ALGORITMA AES ADVANCED ENCRYPTION STANDARD UNTUK ADMINISTRASI REKAM MEDIS".
[11] M. Melina, F. Sukono, H. Napitupulu, and V. A. Kusumaningtyas, "Verifikasi Tanda Tangan Elektronik dengan Teknik Otentikasi Berbasis Kriptografi Kunci Publik Sistem Menggunakan Algoritma Kriptografi Rivest-Shamir-Adleman," *J. Mat. Integr.*, vol. 18, no. 1, p. 27, May 2022, doi: 10.24198/jmi.v18.n1.38343.27-39.
[12] T. Jaringan, A. Hermawan, E. Iman, H. Ujianto, T. Informasi, and U. Teknologi, "InfoTekJar : Jurnal Nasional Informatika dan Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," vol. 2, 2021.
[13] J. D. Bandung, "Ilmiah Komputer dan PENERAPAN DIGITAL SIGNATURE DAN KRIPTOGRAFI PADA Teknik Informatika – Universitas Komputer Indonesia Ilmiah Komputer dan," vol. 6, no. 2, 2017.
[14] W. Hamzah, "Simulasi Dan Analisis Performansi Teknik Rivest Shamir Adleman (RSA) Pada Steganografi Least Significant Bit (LSB)," 2022.
[15] B. Wicaksana and mun Setiawan, "Penerapan Algoritma Advanced Encryption Standard (AES) untuk Pengamanan Berkas Soal Ujian," vol. 10, no. 1, pp. 25–34, 2020, doi: 10.36350/jbs.v10i1.
[16] A. Teguh Utomo and R. Pradana, "IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES-128) UNTUK ENKRIPSI DAN DEKRIPSI FILE," 2022.
[17] Y. Liu, K. Li, Z. Huang, B. Li, G. Wang, and W. Cai, "EduChain: A Blockchain-based Education Data Management System," Jun. 2023, doi: 10.1007/978-981-33-6478-3_5.

Taris Monica

ORIGINALITY REPORT

13%	8%	10%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Rajiv Gupta, Devendra Deshmukh, Awanikumar P. Patil, Naveen Kumar Shrivastava, Jayant Giri, R.B. Chadge. "Recent Advances in Material, Manufacturing, and Machine Learning - Proceedings of 1st International Conference (RAMMML-22), Volume 1", CRC Press, 2023 Publication	1%
2	Submitted to Universitas Amikom Student Paper	1%
3	Seong Oun Hwang, Intae Kim, Wai Kong Lee. "Modern Cryptography with Proof Techniques and Applications", CRC Press, 2021 Publication	1%
4	access.redhat.com Internet Source	1%
5	www.ijitee.org Internet Source	1%
6	www.ece.arizona.edu Internet Source	1%

7	ieomsociety.org Internet Source	1 %
8	Chengliang Liang, Ning Ye, Reza Malekian, Ruchuan Wang. "The hybrid encryption algorithm of lightweight data in cloud storage", 2016 2nd International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR), 2016 Publication	1 %
9	journal.yrpipku.com Internet Source	1 %
10	Submitted to Middlesex University Student Paper	<1 %
11	T. Kavitha, M. K. Sandhya, V. J. Subashini, Prasidh Srikanth. "Secure Communication in Internet of Things - Emerging Technologies, Challenges, and Mitigation", CRC Press, 2024 Publication	<1 %
12	dspace.umkt.ac.id Internet Source	<1 %
13	ejournal.unkhair.ac.id Internet Source	<1 %
14	Submitted to Liverpool John Moores University Student Paper	<1 %
	publikasi.dinus.ac.id	

15	Internet Source	<1%
16	Rizky Damara Ardy, Oktaviana Rena Indriani, Christy Atika Sari, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto. "Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5)", 2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS), 2017 Publication	<1%
17	S. Morioka, A. Satoh. "A 10 Gbps full-AES crypto design with a twisted-BDD S-Box architecture", Proceedings. IEEE International Conference on Computer Design: VLSI in Computers and Processors, 2002 Publication	<1%
18	klik.ulm.ac.id Internet Source	<1%
19	Lecture Notes in Computer Science, 2005. Publication	<1%
20	Mukhsin Nuzula, Yuwaldi Away, Kahlil Kahlil, Andri Novandri. "Optimizing Attendance Data Security by Implementing Dynamic AES-128 Encryption", Sinkron, 2024 Publication	<1%

21	Rafiantika Megahnia Prihandini, Robiatul Adawiyah. "ON SUPER (3n+5,2)- EDGE ANTIMAGIC TOTAL LABELING AND IT'S APPLICATION TO CONSTRUCT HILL CHIPER ALGORITHM", BAREKENG: Jurnal Ilmu Matematika dan Terapan, 2023 Publication	<1 %
22	Shahnawaz Khan, K. Thirunavukkarasu, Ayman AlDmour, Salam Salameh Shreem. "A Step Towards Society 5.0 - Research, Innovations, and Developments in Cloud-Based Computing Technologies", Routledge, 2021 Publication	<1 %
23	doaj.org Internet Source	<1 %
24	ijcat.com Internet Source	<1 %
25	www.scirp.org Internet Source	<1 %
26	www.semanticscholar.org Internet Source	<1 %
27	Wildan Dharma Walidaniy, Mike Yuliana, Hendy Briantoro. "Improvement of PSNR by Using Shannon-Fano Compression Technique	<1 %

in AES-LSB StegoCrypto", 2022 International Electronics Symposium (IES), 2022
Publication

28 CISSP, Susan Hansche, John Berti CISSP, Chris Hare. "Official (ISC)2 Guide to the CISSP Exam", Auerbach Publications, 2019 <1%
Publication

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		