JIKO (Jurnal Informatika dan Komputer) Accredited KEMENDIKBUD RISTEK, No.105/E/KPT/2022
Vol. 7, No. 3, December 2024, pp. 175-181 p-ISSN: 2614-8897
DOI: 10.33387/jiko.v7i3.8654 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
Email: [*1] tarismonica@if.unjani.ac.id, [2]asep.hadiana@lecture.unjani.ac.id, [3]melina@lecture.unjani.ac.id

(Received: 20 August 2024, Revised: 22 October 2024, Accepted: 4 November 2024)

Abstract

Data security is essential. Educational question banks at vocational high schools (SMK) contain confidential information that could be misused if not properly secured. This research aims to ensure students question bank data and develop a responsive web platform for 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, while RSA is an encryption algorithm based on using 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. This research shows 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 the RSA and AES 256-bit encryption has an Avalanche Effect level of 49.99%. Apart from that, the system feasibility test using black box testing results shows that the SIFILE system has a percentage level of 100%. It is hoped that the results of this research can serve as a data security system at Pusdikhubad Cimahi Vocational School and other educational institutions to secure the question bank from unauthorized access.

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

**Corresponding Author: Taris Monica*

1. INTRODUCTION

In today's digital era, various organizations, including educational institutions, face increasingly complex and diverse security challenges. Cyber threats, the risk of data leakage, and potential information compromise are major concerns like never before. The rapid development of information and communication technology, as well as widespread globalization, have created a security landscape that is dynamic and full of challenges. However, on the other hand, technological advances also open up new opportunities to develop more sophisticated and effective security solutions [1]. Often, this sensitive data is kept without adequate security measures, making it vulnerable to various threats. Therefore, it is essential to develop and implement a robust security system to protect the integrity and confidentiality of such information [2],[3].

Sekolah Menengah Kejuruan (SMK) Pusdikhubad Cimahi is a private vocational high school located at Jl. Kalidam No. 1, Cimahi Tengah, Kota Cimahi. It was first inaugurated in 1974. Initially known as STM Elektronika, SMK Pusdikhubad was established by the Pusat Pendidikan Perhubungan (PUSDIKHUB TNI-AD) [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 questions to leakage, whether through internal or external misuse. Exam questions are one type of data that must be kept strictly confidential, especially before the exam time arrives. This situation creates a serious risk to the integrity of the educational evaluation process. To secure important data such as question banks, an effective data security technique is needed. One approach that can be implemented is the use of cryptographic techniques, which offer sophisticated solutions to protect the confidentiality and integrity of sensitive information [2].

To address these security issues, effective methods are needed to protect information. One such method is the use of cryptography. This science studies

how to how to keep messages or documents secure and authentic, ensuring they cannot be accessed or read by unauthorized parties [5]. The Advanced Encryption Standard (AES) is a highly secure cryptographic algorithm used as an encryption standard for sensitive information and is widely adopted. 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 [6]. RSA is an encryption algorithm based on the use of a public key, which plays a crucial 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 adequately large key lengths [7]. On the other hand, AES is an encryption block cipher introduced by the National Institute of Standards and Technology (NIST) in 2000. Both 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 [8].

Several studies have examined data security using RSA and AES algorithms. One such study, conducted by Hajra et al. used the RSA-AES algorithm in the E-Supervision system to improve system security. The test results were obtained using black box testing and usability testing methods. Black box testing was used to test the functionality of the system, while usability testing measured the efficiency of encryption and decryption based on file size. The tests showed that the time required to encrypt a file of 1MB-50MB ranged from 0.182 to 0.393 seconds. The decryption test on a file of 1MB-50MB showed a time range of 0.050 to 0.148 seconds. This study concludes that RSA-AES can be effectively used together to secure data [9]. Research by Ankita et al, discusses the importance of communication and data security in today's digital era, where cryptography plays an important role in protecting data from third parties. This study uses one key for encryption and decryption, with different key sizes that provide different levels of security (128-bit, 192-bit, and 256-bit). This study shows that RSA is more secure than AES because it uses two keys, so it is more resistant to attacks. The conclusion of this study is that RSA is considered more secure than AES because it uses a dual-key system, although AES is also a strong algorithm and is widely used in various applications [10]. The research by Veronica, that integrates the Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) algorithms to ensure the security of payment gateway systems. The system development methodology used is the Agile methodology. This research includes measurements of user acceptance and system performance. The results show that the system is well received by users, meets user needs, functions well, and is able to handle transactions simultaneously with adequate performance. The findings from this research can provide valuable input for companies in building their own systems, as well as insight into algorithm implementation techniques and system workflows [11].

Based on previous research, there have been many studies examining data security using the RSA and AES algorithms. However, there is still a lack of research that specifically focuses on question bank security. Therefore, the gap in this research is to apply RSA and AES algorithms on a responsive website platform. The results of this study are expected to improve the security of exam documents in the context of website-based services in educational institutions.

2. RESEARCH METHOD

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

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 Encryption algorithm. The encrypted secret key is then used to encrypt the plaintext into ciphertext using the AES Encryption algorithm.

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

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

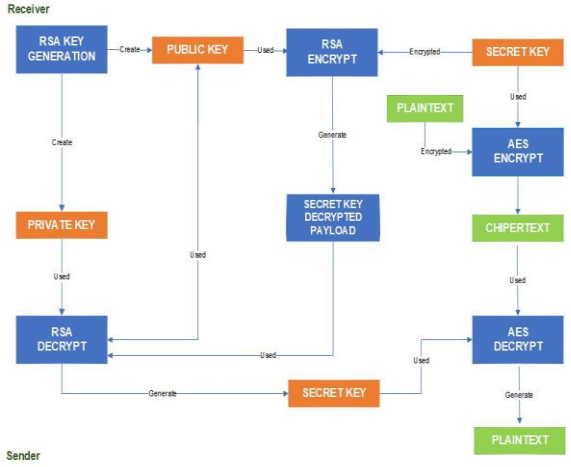

Figure 1. Methodology

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, a use case diagram which provides an overview of the system's behavior when responding to user requests which is further detailed in a use case scenario explaining the system's response. Then, an activity diagram is used by user actors to describe the classification of data managed by the system. Following this, a sequence diagram shows the interactions within the system and between objects, producing specific outputs. After that, a class diagram provides an overview of the system's structure based on the definition of the desired classes created for the system. The final step is to design an interface framework that aims to create an interface aligned with user needs.

2.3 CRYPTOGRAPHY

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

Rivest Shamir Adleman (RSA)

The Rivest-Shamir-Adleman (RSA) cryptographic algorithm was first introduced in 1977 by Ron Rivest, Adi Shamir, and Len Adleman. RSA is a cryptographic algorithm that utilizes asymmetric keys, often referred to as a public key cryptography system. In this algorithm, two keys are used: a public key and a private key. The encryption and decryption processes in RSA are based on the concepts of prime numbers and modular arithmetic. The public key, which is a positive integer, is openly available to the public, while the private key remains confidential and is known only to its owner [12]. In the RSA algorithm involves three main stages or processesor processes that are usually carried out, namely key generation, encryption and decryption. The steps for key generation are [6]:

1. Choose two sufficiently large prime numbers, denoted as 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 Formula 1.

$$n = p \times q \quad (1)$$

3. Calculate the Euler Totien function $\varphi(n)$as the product of $(p-1)$ and $(q-1)$ using Formula 2.

$$\varphi(n) = (p-1) \times (q-1) \quad (2)$$

4. Choose an integer e (usually a prime number that is relatively prime to $\varphi(n)$ and less than $\varphi(n)$) as the public key, using Formula 3.

$$e = \frac{1+\varphi(n)}{d} \quad (3)$$

i is index, d is a prime number less than $\varphi(n)$, and e is public key.

5. Calculate the integer d for the private key using Formula 4.

$$(d \times e)\ mod\ \varphi(n) = 1 \quad (4)$$

d is private key.

Encryption Process

In the encryption process, the plaintext (P) is converted into an integer representation of the message using a mapping scheme, and usually using an ASCII or Unicode table. The encryption process into ciphertext (C) is carried out using Formula 5.

$$C = (P^e)\ mod\ n \quad (5)$$

Decryption Process

The decryption process to return the ciphertext to plaintext is carried out again using Formula 6.

$$P = (C^d)\ mod\ n \quad (6)$$

P is *plaintext*, C is *ciphertext*, d is private key, and n is the result of multiplying prime numbers.

Advanced Standard Encryption (AES)

The Advanced Encryption Standard (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 [13]. AES with a 128-bit key functions as a symmetric key, meaning it uses the same key for both encryption and decryption. Compared to longer AES keys, AES 128 bit works faster and more compact, using fewer rounds to secure data [14].

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, nd then AddRoundKey again. This sequence is repeated for the specified number of rounds. AES is shown in Table 1.

Table 1. AES

Algorithm	Key length (bits)	Block size (bits)	No of round
AES-128	129	128	10
AES-192	192	128	12
AES-256	256	128	14

Authentication

Authentication is the process of validating a user's identity when accessing a system. Its goal is to ensure that the user's identity is legitimate [15].

Encryption Process

The encryption process involves four types of byte transformations in the AES algorithm. First, AddRoundKey applies 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 shifts the bytes in each row of the state array, while the 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 for a certain number of rounds (Nr), which is called the Round Function. In the last round, the state does not undergo the MixColumns transformation.

3. RESULT AND DISCUSSION

The results of software quality and testing include the assessment of the accuracy of the developed machine learning model [17].

3.1 Implementation System

At this stage the focus is on implementing the software according to the design. The implementation is carried out locally using a personal computer to facilitate testing. The software developed is web based, utilizing Hypertext Preprocessor (PH) as the main programming language, Visual Studio Code as the development environment, Google Chrome as the web browser, MySQL as the database, and Apache from XAMPP as the web server.

3.2 Interface Implementation

The implemented system interface is a website that displays the application's home page and encryption page, along with an explanation of the document showing the results of the avalanche effect test, including the file sizes (in bytes) before and after encryption, which were previously uploaded to the website. These elements are shown successively Figure 2,3,4,5,6.

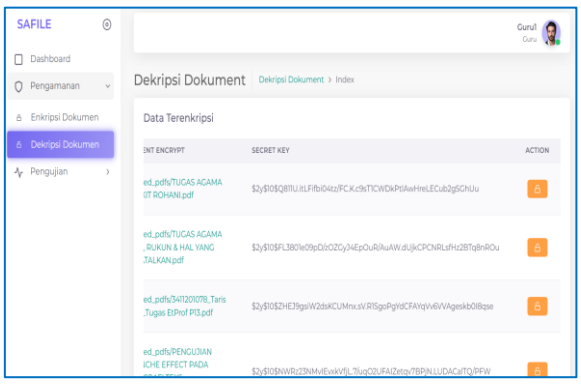

Figure 2. Encryption page

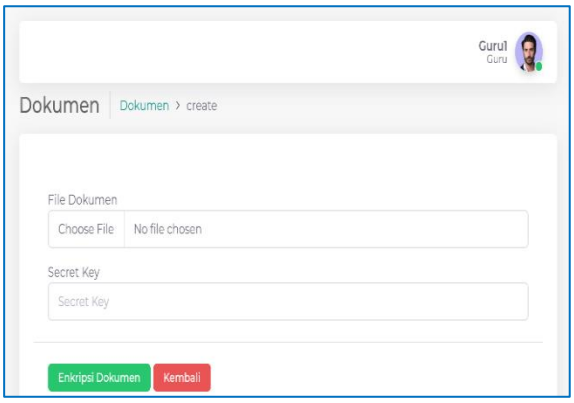

Figure 3. Add question document page

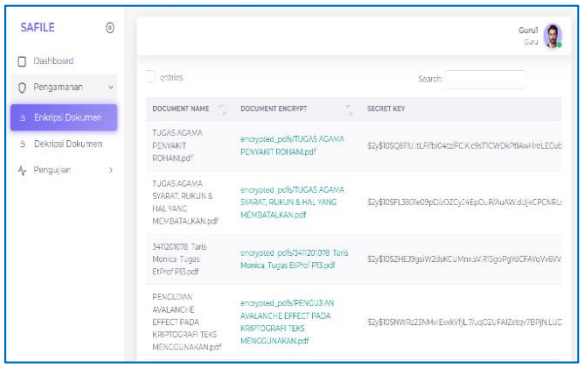

Figure 4. Description Page

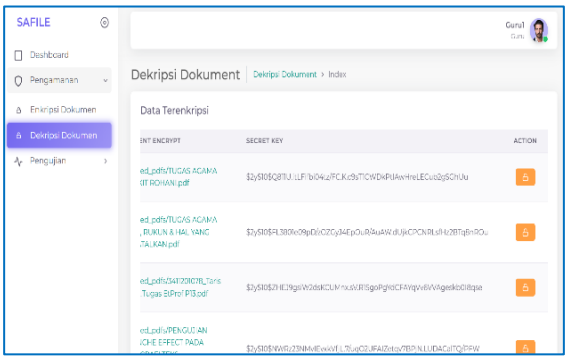

Figure 5. Secret key description form page

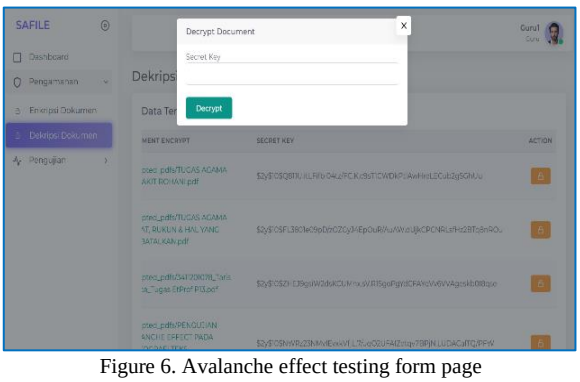

Figure 6. Avalanche effect testing form page

3.3 Testing Software

The results of black box testing on the design of the 'SIFILE Application', indicate that all features function according to the design specifications. 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 (NT): 4 test codes
2. Corresponding result test code (CR): 4 test codes
3. Unsuitable result test code (UR): 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 Formula 7.

$$Result = \frac{NT-UR}{CR} \times 100\% \quad (7)$$

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

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.

3.4 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 2. Blackbox testing

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

3.5 Avalanche Effect Test Result

Avalanche Effect (AE) testing is conducted 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 are illustrated in Figures 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

3. Experiment-3 (Change the last 1 character)
   Before smk pusdik hubad
   After smk pusdik hubaa
   c. Chiper Text
   Before ffvC7zSAPpLY6I9yixXvkqAGXXVAVyihBLaJPaCqWPc=
   After vuFqK5svWmfRyP7HOfuKZhj0s7HYyBIkbXqMiAUU378=
   d. 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 10111110 11100001 01101010 00101011 10011011 00101111 01011010 01100111 11010001 11001000 11111110 11000111 00111001 11111011 10001010 01100110 00011000 11110100 10110011 10110001 11011000 11001000 00011001 01100100 01101101 01111010 10001100 10001000 00000101 00010100 11011111 10111111
   e. Calculation Avalanche Effect

$$Avalanche\ Effect = \frac{130}{256} \times 100\% = 50{,}78\%$$

Figure 9. Example 3 avalanche effect testing

Table 3. 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 three experiments conducted, the Avalanche Effect (AE) values obtained were 48.04% in the first experiment, 51.17%, in the second experiment, and 50.78% in the third experiment. The calculated average value is 49.99%. This average value indicates that the AE test is adequate, as it falls within the acceptable range of 45% to 60%. Based on the avalanche effect test results, the average value obtained for the question document was 30.48%. This result indicates that the AES cryptographic algorithm demonstrates a good avalanche effect, as significant changes in plaintext lead to noticeable changes in ciphertext, affecting multiple bits. However, the test results show that using a more complex secret key (including spaces, numbers, and characters) does not significantly impact the encryption results of the question document, as reflected by the avalanche effect value.

4. 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 have 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.

5. REFERENCE

[1] E. Jackson and O. Mardner, "Education And Security Current And Future Challenges In Teaching And Learning Security Studies," *Conf. Secur. Horizons*, pp. 49–54, Sep. 2022, doi: 10.20544/ICP.3.6.22.P04.

[2] B. Wicaksana and M. Setiawan, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Pengamanan Berkas Soal Ujian," *TeknoIS J. Ilm. Teknol. Inf. dan Sains; Vol 10, No 1 MeiDO - 10.36350/jbs.v10i1.74* , May 2020, [Online]. Available: http://teknois.unbin.ac.id/index.php/JBS/article/view/74.

[3] M. Dzikri Azhari Ali, Asep Id Hadiana, "Teknik Pengamanan Data Menggunakan Algoritma Advance Encryption Standard Dengan Common Event Format Untuk Meningkatkan Keamanan Log Jaringan," *INTECOMS J. Inf. Technol. Comput. Sci.*, vol. 7, 2024.

[4] Alfian Rahman, Ade Kania Ningsih, and Ridwan Ilyas3, "Penggunaan QR Code Berbasis Kriptografi Algoritma Advanced Encryption Standard Dan Sha-512 Untuk Aplikasi Pencatatan Biaya Pendidikan Berbasis Web Di Smk Pusdikhubad," *Sci. J. Ilm. Sains dan Teknol.*, vol. 2, no. 3 SE-Articles, pp. 205–217, Feb. 2024, doi: 10.572349/scientica.v2i3.1137.

[5] B. C. Ashari and S. Waluyo, "Pengamanan File Ujian Menggunakan Algoritma Advanced Encryption Standard 128 Di SMP Negeri 22," *Pros. Semin. Nas. Mhs. Fak. Teknol. Inf.*, vol. 1, no. 1 SE-Cyber Security, pp. 240–247, Sep. 2022, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/article/view/198.

[6] F. Farhan and D. Leman, "Implementasi Metode Rivest Shamir Adleman (RSA) Untuk Kerahasiaan Database Perum Bulog Kanwil SUMUT ," *J. Mach. Learn. Data Anal.*, vol. 2, no. 1 SE-Articles, Feb. 2023, [Online]. Available: https://journal.fkpt.org/index.php/malda/article/view/483.

[7] J. Hutagalung, P. Ramadhan, and S. Sihombing, "Keamanan Data Menggunakan Secure Hashing Algorithm (SHA)-256 dan Rivest Shamir Adleman (RSA) pada Digital Signature," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, pp. 1213–1222, Dec. 2023, doi: 10.25126/jtiik.1067319.

[8] A. N. Agustina, A. Aryanti, and N. Nasron, "Pengamanan Dokumen Menggunakan Metode Rsa (Rivest Shamir Adleman)berbasis Web," *Seminar Nasional Multi Disiplin Ilmu Unisbank 2017*. Indonesia, 2017.

[9] H. Ngemba, A. Anand, S. Hendra, A. Kasim, and E. Chandra, "E-Surveillance System Security Using RSA-AES Algorithm (Rivest Shamir Adleman - Advanced Encryption Standard)," *Tadulako Sci. Technol. J.*, vol. 5, pp. 22–32, Jun. 2024, doi: 10.22487/sciencetech.v5i1.17175.

[10] A. Chandel, A. Aggarwal, A. Mittal, and T. Choudhury, "Comparative Analysis of AES & RSA Cryptographic Techniques," in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, 2019, pp. 410–414, doi: 10.1109/ICCIKE47802.2019.9004338.

[11] Veronica, R. Oetama, and A. Ramadhan, "Incorporating rivest-shamir-adleman algorithm and advanced encryption standard in payment gateway system," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 22, pp. 629–644, Apr. 2024, doi: 10.12928/TELKOMNIKA.v22i3.25578.

[12] 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, p. 27, May 2022, doi:

10.24198/jmi.v18.n1.38343.27-39.
[13] 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.
[14] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Inform.*, vol. 8, p. 52, Sep. 2018, doi: 10.30864/eksplora.v8i1.139.
[15] Y. Liu, K. Li, Z. Huang, B. Li, G. Wang, and W. Cai, "EduChain: A Blockchain-Based Education Data Management System," 2021, pp. 66–81.
[16] A. Teguh Utomo and R. Pradana, "Implementasi Algoritma Advanced Encryption Standard (Aes-128) Untuk Enkripsi Dan Dekripsi File," 2022.
[17] M. Melina, Sukono, H. Napitupulu, and N. Mohamed, "Modeling of Machine Learning-Based Extreme Value Theory in Stock Investment Risk Prediction: A Systematic Literature Review," *Big Data*, pp. 1–20, Jan. 2024, doi: 10.1089/big.2023.0004.