Journal of Technology and Computer (JOTECHCOM)
Vol. 2, No. 4, November 2025, pp. 260~267
ISSN: 3048-0477 (Media Online)

Implementation of Security on Library System Login Using a Combination of AES and RSA Cryptography

M. Zaki Musaid Siregar
Engineeringand Computer Science, Informatic Engineering, Universitas Harapan,Medan, Indonesia
zakimusaid04@gmail.com

Article Info

Article history:

Received October 07, 2025
Revised November 15, 2025
Accepted November 26, 2025

Keywords:

AES
Cryptography
Digital Library
RSA
System Security

ABSTRACT

The development of information technology has encouraged library systems to shift from manual methods to digital-based platforms. While this transformation improves efficiency, it also raises security risks in the login process, which handles sensitive user data. This research aims to implement login security using a combination of the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms. AES-128 is used to encrypt passwords, while RSA is used to encrypt the AES output before transmission to the server. The research method includes requirements analysis, security architecture design, algorithm implementation, and testing through login simulations and traffic analysis using Wireshark. The results show that the combination of AES and RSA effectively protects user credentials and prevents unauthorized access to the transmitted data. The conclusion of this study is that the combined cryptographic approach provides dual protection for library system authentication. Further development is suggested by integrating secure communication protocols such as HTTPS and exploring modern public-key cryptographic algorithms.

Corresponding Author:

M Zaki Musaid Siregar
Universitas Harapan Medan
Email: zakimusaid04@gmail.com

1. INTRODUCTION

Advances in information technology have made many areas easier, including library management. Digital library systems are becoming more common because they are more efficient and practical than manual systems. Users can search for, borrow, and return books online. However, the use of digital systems poses new challenges, especially regarding data security. User information such as names, identities, and borrowing histories must be protected from misuse or theft. Therefore, the security of the login process in library systems is very important.

A digital library is a software system that professionally integrates printed and non-printed works. Its purpose is to support research, education, preservation of library materials, information retrieval, and recreation for the general and specialized public. Although it does not always have a physical form, a digital library can be accessed via devices such as computers or mobile phones, and the system can be tailored to the needs of library users. However, many such systems do not yet have adequate security. As a result, the system is vulnerable to password theft, data interception, and illegal access. There are also systems that do not properly encrypt login data, so that in the event of a breach, user data can be easily read. This problem shows that login data security is a major weakness that needs to be addressed in the development of digital libraries. [1].

To address security issues in login systems, one solution that can be used is cryptography. Cryptography is the mathematical science of transforming data so that its meaning cannot be understood,

preventing unauthorized changes, or preventing unauthorized use [2]. Two cryptographic algorithms commonly used in information security are AES and RSA. AES is a symmetric algorithm that is secure enough to protect confidential data; the same key is used for encryption and decryption. Meanwhile, RSA is an asymmetric algorithm, where the key used for encryption (public key) is different from the key used for decryption (private key) [3].

From the issues discussed, it can be concluded that security in the login system of digital libraries must be taken seriously. User data needs to be protected so that it is not misused by irresponsible parties. For this reason, the use of cryptography especially a combination of AES and RSA algorithms is an important solution. This topic was chosen because it is very useful for improving information system security and building a more reliable and trustworthy library. In addition, this research can be used as a reference for other systems that also need comprehensive user data protection.

2. METHOD

2.1 Cryptography

Cryptography has another meaning, namely a science that studies mathematical techniques related to data security or message security using two basic cryptographic processes, namely encryption and decryption. Encryption can be defined as a cipher or code, which is the process of hiding a data message by converting plaintext (a readable message) into ciphertext (a random message that cannot be read), while decryption is the opposite of encryption, which is converting the disguised form back into the original information [4].

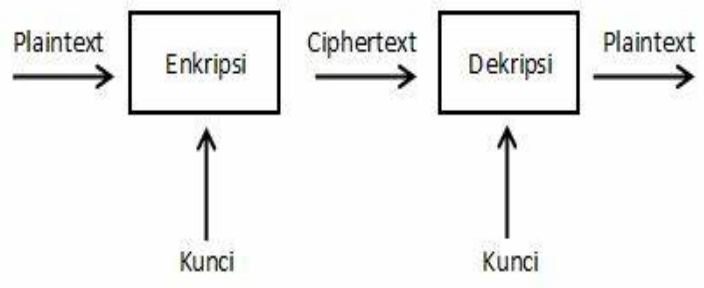

Figure 1. Encryption & Decryption Process

The main purpose of cryptography is to maintain information security by ensuring that data can only be accessed by authorized parties. The main objective of cryptography in the context of information security covers several core aspects known as the pillars of security. Confidentiality, Integrity, and Availability are complemented by other important elements such as Authentication and Non-repudiation [5].

2.2 Rivest-Shamir-Adleman (RSA)

The RSA cryptography algorithm was created by three researchers from MIT (Massachusetts Institute of Technology), namely Rivest, Shamir, and Adleman, in 1976. The three of them came together to create and research the cryptographic algorithm with different educational backgrounds at the Artificial Intelligence LAB on the MIT campus. Finally, the RSA Cryptography Algorithm was created, and the name RSA stands for the combination of the names of those who created and researched it: R = Rivest, S = Shamir, and A = Adleman [6].

The RSA cryptographic algorithm is designed to generate keys that are used for encryption that are different from the keys used for decrypting messages. The RSA algorithm is a data security technique that matches the public key owned by the sender of the document with that of the recipient of the document, which is then decrypted using a private key. The private key is a key used to decrypt messages that not everyone is allowed to know; only certain people who have the right to decrypt messages can do so [7]. The steps for creating a key are as follows:

1. The initial procedure in the RSA algorithm is to select two prime numbers p and q. Both must be prime numbers and not the same value.
2. Multiply p and q to produce the value n.
3. Create a public key e that is relatively prime to m, where $m = (p - 1)(q - 1)$.
4. To obtain the private key d, calculate the values p, q, e, using the congruence $ed = 1 \bmod m$.

Encryption, converting the original message into code, is the core of cryptography. Therefore, the purpose of key expansion is to be able to encrypt messages with the public key that has been obtained. Here is the encryption formula and process:

$$C=M^e \pmod n$$

The recipient uses a private key to retrieve the message. To restore the original message, we take the encrypted message that we obtained earlier and decrypt it using the following formula:

$$M= C^d \pmod n$$

2.3 Advance Encryption Standart (AES)

The Advanced Encryption Standard (AES) is a symmetric encryption standard used to protect sensitive information. AES is one of the most widely used encryption algorithms worldwide and has been widely adopted by governments, industries, and other organizations to protect sensitive data. AES cryptography can also secure data content such as databases [8]. The four basic AES operations are designed based on classical cryptography principles, namely confusion and diffusion, introduced by Claude Shannon. SubBytes and AddRoundKey contribute to confusion by complicating the relationship between the key and the ciphertext. Meanwhile, ShiftRows and MixColumns aim to increase diffusion, so that small changes in the plaintext or key will result in large and widespread changes throughout the ciphertext [9].

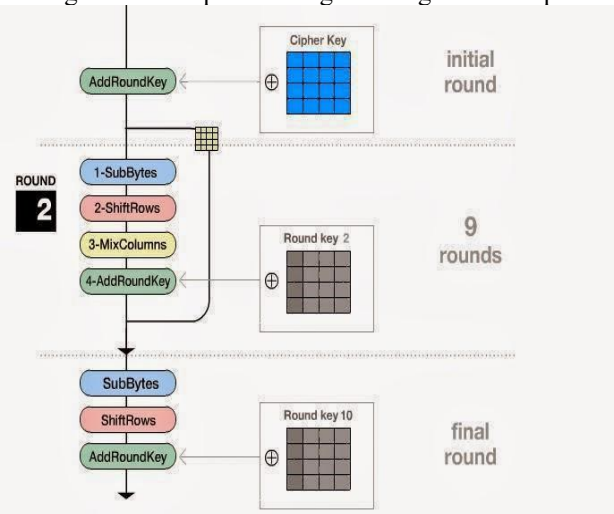

Figure 2. AES Algorithm Encryption Process

The Advanced Encryption Standard algorithm is a symmetric algorithm, which means that the encryption and decryption processes use the same key [10] The following is a general explanation of the encryption process in the Advanced Encryption Standard algorithm:

1. Initial round (AddRoundKey)
   AddRoundKey is the initial operation in the AES algorithm, performed before the main rounds. This is an important step because it introduces the key to the initial data (plaintext), initiating the strong encryption process. AddRoundKey performs an XOR between the initial state (plaintext) and the cipher key.
2. Main round
   Each main round consists of four main stages, with Nr – 1rounds. The process carried out in each round.
   1) SubBytes
      byte substitution using a substitution table (S-box).
   2) ShiftRows
      ShiftRows is a row permutation transformation (permutation step).
   3) MixColumns
      MixColumns performs a linear transformation on each column (4 bytes) of the state matrix.
   4) AddRoundKey
      The state resulting from MixColumns is XORed with the round key.
3. Final Round
   The final stage or final round is the last stage in the AES encryption process, and has a sequence of operations that is almost the same as the main round, but without the MixColumns operation.

3. RESULT AND DISCUSSION

A crucial stage in the information system development cycle, where the design created in the previous stage is realized into a system that can be run and tested. In this study, the implementation focuses on the application of the Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) cryptography algorithms in the user authentication (login) process in the library information system.

3.1 AES & RSA Cryptography Flowchart

The flowchart explains how the system decrypts the AES key using the RSA private key, which is then used to decrypt the previously encrypted password. The decrypted password will be matched with the data stored in the database to determine the validity of the user's login. If the data matches, the user is granted access to the library system; otherwise, the system will display an error message. The system flowchart not only describes the sequence of technical processes, but also explicitly shows how the system implements multi-layered data security. This diagram can also be used as a primary reference in the debugging process, system testing, and further development (system scaling), because it is functionally capable of showing critical points in the processing of sensitive data.

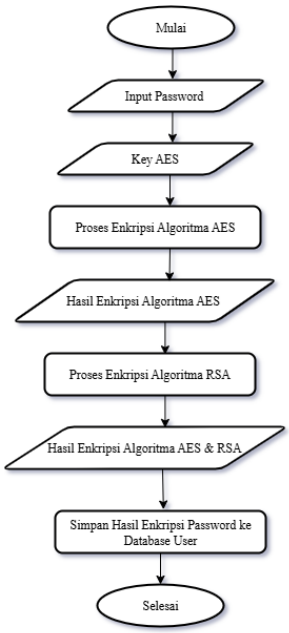

Figure 3. AES & RSA Cryptography Flowchart

3.2 Login Program Flowchart

The program flowchart focuses more on the flow of instructions at the program or code level. In this system, the login process is not carried out directly without security, but is arranged through complex yet efficient cryptographic stages. When the user enters their username and password, the system will encrypt the password using the AES algorithm. The password in ciphertext form will not be directly compared with the data in the database.

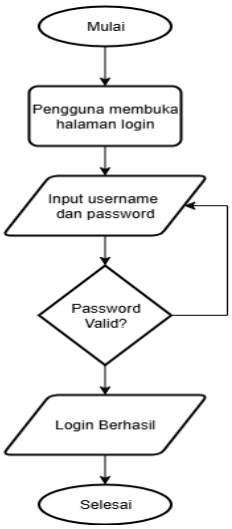

Figure 4. Login Flowchart

3.3 Login System Components

The login system is a core part of the security system in this library application, where users must go through an authentication process before they can access the system's features. In its implementation, the login process not only includes matching usernames and passwords, but also involves a cryptography-based security mechanism, which is a combination of Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA). The following are the main components that make up the login system structure:

1. Login Form (Frontend)
   This form is a user interface that allows users to enter their username and password. The data entered is not sent directly to the server, but is first processed cryptographically.
2. AES Encryption Module (Client-side or Server-side)
   User passwords are encrypted using the AES-128 algorithm with a predetermined secret key. AES is used because of its speed and efficiency in handling small-dimensional data such as passwords.
3. RSA Encryption Module (Client-side)
   The result of the AES encryption is then encrypted again using the server's RSA public key. This process ensures that only the server can decrypt the result using the RSA private key.
4. Server (Backend Processing) The server receives the encrypted data and performs a gradual decryption process: first RSA decryption, then AES decryption. The final result is compared with the encrypted data stored in the database.
5. Database (Encrypted Password Storage) The system does not store users' original passwords. Passwords are stored in the form of AES-encrypted ciphertext that cannot be read without a valid decryption process.

3.4 User Database Results

The following is a display of the user database where the results of AES and RSA encryption converted to base64 will be entered into the user database.

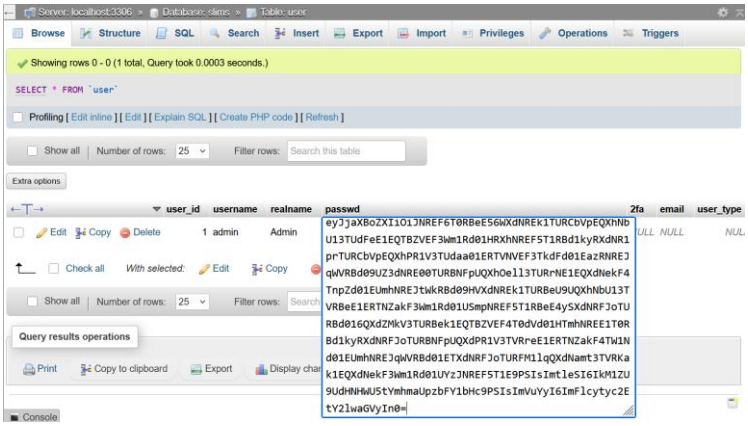

Figure 5. User Database Display

3.5 SLiMS Main Page Display

The following is the main page display on the SliMS application, which can be seen below:

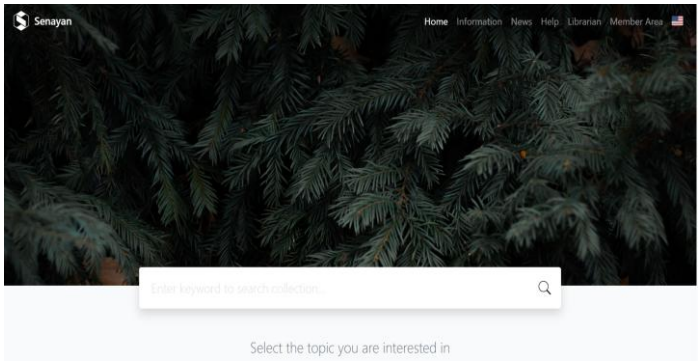

Figure 6. SliMS Home Page

3.6 Login Page Display

Showing the library system interface that combines the encryption process in the authentication flow. When users enter their credentials, both the username and password are first processed through encryption algorithms such as AES (symmetrical) and RSA (asymmetrical) before the system verifies the data's validity. The following is a user interface display for the library system login page that has been integrated with the encryption process, as shown in the image below:

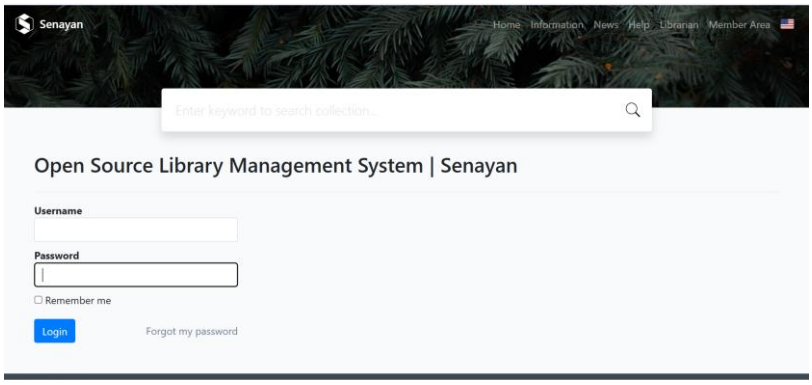

Figure 7. Login Page

3.7 Page Display After Successful Login

The following is the page display after successfully logging in, which can be seen in the image below:

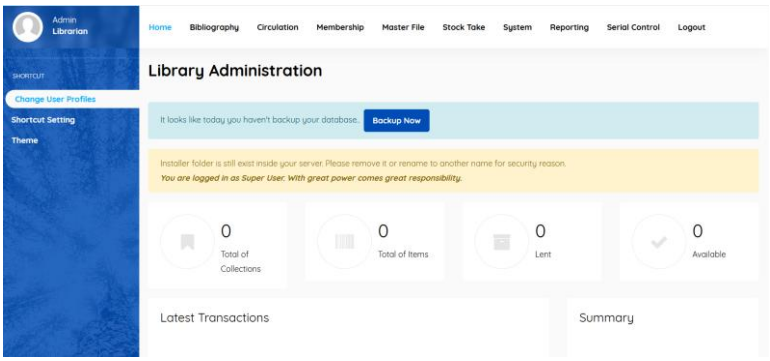

Figure 8. Page After Successful Login

3.8 Failed Login Page Display

Displaying a failed authentication interface (login failed), where the system clearly displays a striking error message (pink background with the text 'Wrong Username or Password. ACCESS DENIED') above the login form without redirecting the user to a new page. The following is a view of the page when a login fails (unable to log in), which can be seen in the image below:

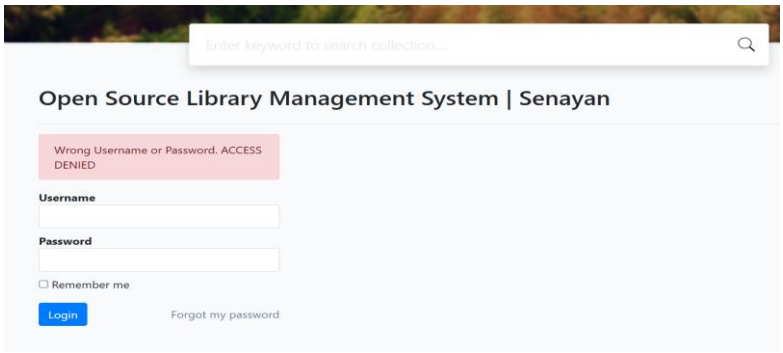

Figure 9. Login Page Display Failed

3.9 Test Results

The test results involved two areas of analysis: manual computation and system testing. Both stages use a double encryption approach, where the plaintext "LOGINPERPUSTAKAN" is first encrypted with the Advanced Encryption Standard (AES) algorithm, then the encrypted result is re-encrypted with the Rivest–Shamir–Adleman (RSA) algorithm. The results obtained from this process are then systematically summarized in a table, showing a comparison between the values obtained manually, including the AES and RSA encryption processes in stages, with the output generated by the automatic system in the actual implementation.

4. CONCLUSION

By designing a login system for the Library Information System using a combination of AES and RSA algorithms, security functions are separated into two layers. AES efficiently encrypts credential data, while RSA secures the distribution of AES keys so that they are not leaked during transmission. During authentication, the username and password are first encrypted, then the AES session key, which is randomly generated during each login process, is encrypted using RSA so that only the server is able to decrypt and validate the data. Practical results show that this security layer significantly improves protection against attacks such as man-in-the-middle, eavesdropping, and brute force, while ensuring that passwords are never sent in plaintext, making the authentication method more secure than conventional methods.

ACKNOWLEDGEMENTS

First of all, the author would like to express gratitude for completing this article and research. The author would like to express his deepest gratitude to his supervisor for providing guidance and motivation so that the author could complete this research well. The author realizes that this research still has many shortcomings and needs to be developed further.

REFERENCES

[1] Rafi Ramadhan, "Pengelolaan Perpustakaan Digital Di Badan Perpustakaan Dan Kearsipan Daerah Provinsi Jawa Barat," *J. Pustaka Budaya*, vol. 10, no. 1, pp. 21–31, 2023, doi: 10.31849/pb.v10i1.11270.

[2] Tuti, "Hakikat Dan Karakteristik Filsafat Dan Filsafat Ilmu," vol. 1, no. 2110247655, pp. 42–46, 2022.

[3] I. Dan, A. Kombinasi, and A. E. S. Dan, "IMPLEMENTATION AND ANALYSIS OF THE COMBINATION OF RSA , AES AND STEGANOGRAPHY IN THE ENCRYPTION OF URBAN," vol. 3, no. September, pp. 20–29, 2024.

[4] N. A. Nanda, S. M. S. Silalahi, D. Fatricia Nasution, M. Sari, and I. Gunawan, "Kriptografi dan Penerapannya Dalam Sistem Keamanan Data," *J. Media Inform.*, vol. 4, no. 2, pp. 90–93, 2023, doi: 10.55338/jumin.v4i2.428.

[5] Y. S. Anwar, A. Abdillah, and S. Sirajudin, "Mengenal kriptografi sejak dini: membangun kesadaran keamanan data pribadi," *SELAPARANG J. Pengabdi. Masy. Berkemajuan*, vol. 9, no. 4, pp. 2028–2033, 2025.

[6] N. Berliano Novanka Putra, F. Amalia Raihana, W. Michael Albert Mondong, A. Rosadi Kardian, P. Siber dan Sandi Negara, and J. Barat, "Analisis Enkripsi Kriptografi Asimetris Algoritma RSA Berbasis Pemrograman Batch pada Media Flashdisk," *J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 8, no. 1, pp. 142–154, 2023, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

[7] R. S. Y. Simbolon and P. D. Silitonga, "Pengamanan Data Dengan Menggunakan Teknik Kriptografi Public Rsa Dan Knapsack," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 03, no. 01, pp. 9–12, 2021, doi: 10.54367/kakifikom.v3i1.1195.

[8] I. Gunawan, "Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force," *TECHSI - J. Tek. Inform.*, vol. 13, no. 1, p. 14, 2021, doi: 10.29103/techsi.v13i1.2395.

[9] F. Yusri *et al.*, "Implementasi Algoritma Advanced Encryption Standard (AES) Secara Manual Menggunakan Python," *JIKUM J. Ilmu Komput.*, vol. 1, no. 1, pp. 12–16, 2025, doi: 10.62671/jikum.v1i1.38.

[10] W. Putra, M. R. Fahlevi, and A. T. Hidayat, "Implementasi Algoritma Advanced Encryption Standard Untuk Kemanan Dokumen," *J. Ilmu Komputer, Teknol. Dan Inf.*, vol. 1, no. 2, pp. 76–83, 2023, doi: 10.62866/jurikti.v1i2.55.