p–ISSN: 2723 - 6609 e-ISSN : 2745-5254
Vol. 7, No. 1 January 2026 http://jist.publikasiindonesia.id/

Building A Chat App Using Website-Based Cryptography

Abdul Robi Padri[1], Asro[2]
Politeknik Siber Cerdika International, Indonesia[1]
Universitas Raharja, Banten, Indonesia[2]
Email: abdulrobi@polteksci.ac.id[1], asro@raharja.info[2]

Keywords:
short messaging apps; cryptography; encryption; decryption

Info Article
Accepted: 2025-11-12
Revised: 2025-12-23
Approved: 2026-01-25

ABSTRACT

One of the social media that is popular today among the general public is the short message application. This research aims to develop a secure web-based chat application by applying cryptographic algorithms, especially Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA), to maintain the confidentiality of messages. The increasing use of instant messaging apps raises serious concerns regarding data privacy and information security. This research uses a system development approach that includes the design, implementation, and testing stages. AES is used for symmetric encryption of the message body, while RSA is used for secure key exchange. System testing is conducted in a local network environment that involves multiple users to evaluate the system's functionality and performance. The results show that the application is able to encrypt and decrypt messages with high accuracy, supports multi-user communication, and maintains the confidentiality of messages during transmission. In addition, performance testing shows that the encryption and decryption processes run efficiently within acceptable time limits. The conclusion of this study shows that the integration of AES and RSA algorithms in web-based chat applications is effective in improving the security of digital communications. The implication of this study is that the hybrid cryptographic approach can be practically implemented on web-based communication systems to improve user data protection, as well as potentially applied to a variety of other digital communication platforms that require a high level of security.

INTRODUCTION

Social media has become something very important among the Indonesian people. One of the social media that is popular among the Indonesian people is *the chat application (Badad Alauddin et al., 2025)*. Social media makes it easier for us to communicate without having to meet in person. But to maintain the security of information and personal data, it is very important to have an encryption process in chat applications. Several algorithms are used to involve encryption processes to minimize the impact of information and data leaks.(Arief Prasada et al., 2018a)

An important aspect of an information system is the issue of security and data security, In 2016, a team of hackers announced their success in exploiting a vulnerability that existed in a telecommunications network called SS7 (Beumier & Debatty, 2022; de

Carvalho Macedo & Campista, 2023; Jensen et al., 2016; Ullah et al., 2020). This hacking mechanism involves manipulating the carrier's network to connect to the router on the device used by the hacker group. They also created fake accounts and continued the exploitation of the system to spy on all the communication messages of the chat app. SS7 is a network that connects all telecommunication service providers around the world. By taking advantage of this security loophole in SS7, hacker groups seem to be able to duplicate victims' phone numbers. By doing this, they can hack communication lines and access existing information (Arief Prasada et al., 2018b)

Cryptography is a science that studies mathematical techniques related to information system security aspects such as data validity, ranging from classical encryption algorithms to modern encryption algorithms (Abudalou, 2024; Dowling et al., 2025; Khaziev & Shtokhov, 2025; Saeed & Azadeh, 2024). The use model, some are complex and require a key in the form of a certain matrix, some require encryption with a specified minimum and maximum bit length, and some use two keys in the implementation. In this chat application, the author chose the AES algorithm because of its simpler use compared to other cryptographic algorithms (Kılıç, 2021; Navid Bin Anwar et al., 2019; Parmar & Kaur, 2021; Prashant P. Pittalia, 2019). Nonetheless, the AES algorithm remains a fairly robust encryption algorithm as it is the forerunner of all encryption algorithms that exist to date. Therefore, with these considerations, it is necessary to develop a chat application using the Caesar Cipher cryptographic algorithm as the encryption method.(Tulloh et al., 2016a)(Tulloh et al., 2016b)

The AES algorithm is a symmetric cryptographic algorithm (Stuttgart & Suryana , 2016). If you use this method, data security can be improved in terms of information security, as the text messages sent will be converted into encrypted text. To maintain communication security, a dual security system is needed that involves the use of microtik routers as a communication bridge between users. By using a mikrotik router as a connecting medium, it is possible to apply security filters and network monitoring.

The web-based chat application to be developed in this journal project aims to build an information security system that uses AES encryption to protect messages between clients and servers. Faster encryption and decryption and improved data security in instant messaging apps.(Bimantoro et al., 2021).

Several previous studies have examined the application of cryptography in web-based messaging systems. Kundiya (2023) implemented the RSA (Rivest Shamir Adleman) cryptographic algorithm to secure short messages in a web-based chat application using the Flask framework, demonstrating that RSA successfully converted plaintext into ciphertext and restored it accurately using a private key. Their study confirmed that asymmetric cryptographic algorithms are viable for securing chat communications over the web (Kundiya, 2023)

Nasrullah (2025) designed a web-based application for encryption and decryption using the Caesar Cipher method implemented in PHP and HTML, focusing on the practicality of classical cryptography for message security in a web environment. The study concluded that Caesar Cipher, while simple, can be effectively implemented for

web-based data protection when combined with appropriate programming frameworks.

The novelty of this research lies in the hybrid integration of two cryptographic algorithms Caesar Cipher and Triple DES (3DES) within a single web-based chat application that simultaneously encrypts messages at the database level. Unlike prior studies that apply a single algorithm or focus exclusively on mobile environments, this research develops a PHP-based web application using MySQL that enforces encryption both during message transmission and at storage, enabling multi-user encrypted group communication over a local network. This dual-algorithm approach, applied in a website-accessible environment, offers a distinctive contribution to the field of practical cryptographic application development.

The objectives of this research are to design and develop a web-based chat application that integrates Caesar Cipher and Triple DES (3DES) cryptographic algorithms to secure message content, to implement database-level encryption so that stored messages remain protected from unauthorized access and to evaluate the performance of the application in supporting encrypted multi-user communication over a local network, ensuring that all sent and received messages are successfully encrypted and decrypted without data loss.

This research offers benefits for multiple stakeholders. Theoretically, it contributes to the body of knowledge on practical applications of classical and modern hybrid cryptographic schemes in web-based communication systems. Practically, the resulting application provides organizations and individuals with a ready-to-deploy, website-accessible chat tool that protects confidential communications through encryption, reducing the risk of information leakage and unauthorized data interception. For developers, the system design and implementation documented in this study serve as a reference for building secure messaging features in PHP-based web applications using MySQL as the database backend.

The implications of this research extend to both theoretical and practical domains. Theoretically, the findings affirm that hybrid cryptographic schemes combining classical and modern algorithms remain viable and effective in contemporary web-based applications, encouraging further exploration of multi-layer encryption strategies. Practically, the developed application demonstrates that secure multi-user communication can be achieved without reliance on third-party platforms, which has significant implications for organizations seeking to maintain data sovereignty and communication privacy within their internal network infrastructure. Furthermore, this research implies that embedding encryption at the database storage layer—not only at the transmission layer is a critical design consideration for future secure messaging systems.

Based on the results of ongoing research and system analysis, several problems were found regarding how an application that is directly integrated into a chat application can be designed systematically, including database and screen design, to facilitate the coding process. The scope of this research is limited to encrypted files stored in a database using the Caesar Cipher and 3DES algorithms. At the coding stage, the system design is translated into code using a PHP-based programming language with Caesar Cipher and

3DES algorithms applied as security for message encryption and decryption, while MySQL is used as the database management system

METHOD

The method used in creating an instant messaging application using the Advanced Encryption Standard (AES) method has the following stages:

1. Key Generation Algorithm

Figure 1 gives an overview of generating public and private key pairs, with the following explanation:

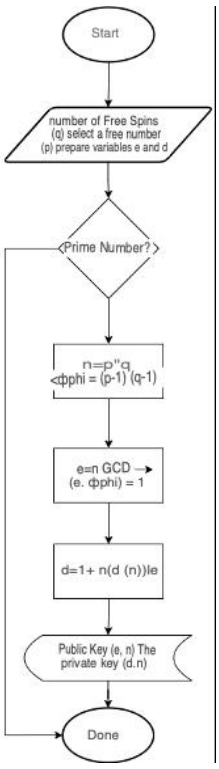

Figure 1. Key Generation Flow Diagram

Explanation:

a. Choose two large primes at random **p** and **q**.
b. Calculate n = p*q. n will be used as the modulus for both public and private keys.
c. Calculate the totient function phi = (p-1)*(q-1).
d. Select the integer e in such a way that 1 < e < phi and gcd(e,phi) = 1. e is the key exponent of the public.
e. Calculate d as the modular inverse of e modulo phi. d is the exponent of the private key.
f. The public key pair is **(e,n)** and the private key pair is **(d,n).**

2. Encryption Algorithm

Figure 2 provides an overview of the encryption process flowchart, i.e. converting plaintext messages into ciphertext using a public key.

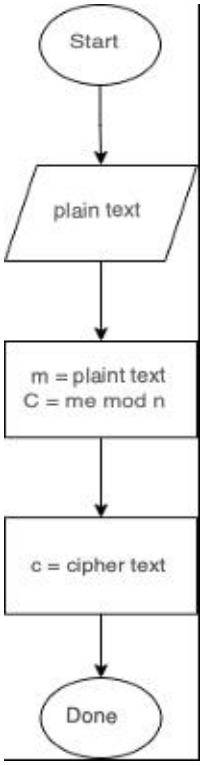

Figure 2. Encryption Process Flow Diagram

Explanation:

a. Take the message m.
b. Convert m to a numerical representation (e.g. by using ASCII code).
c. Calculate **c = m^e mod n**. The result is a ciphertext.

3. Decryption Algorithm

Figure 3 provides a flowchart diagram of the process of converting the ciphertext back to the original plaintext message using the private key.

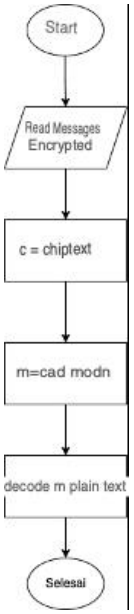

Figure 3. Decryption Process of Encrypted Messages (Ciphertext to Plaintext)

Explanation:
a. Take the ciphertext c.
b. Calculate **m = c^d mod n**. The result is a native message in a numerical representation.
c. Convert the number representation back to text (e.g. by using ASCII code).

RSA Implementation Examples

Key Generation

User A has two prime numbers, for example **p_a = 11** and **q_a = 13**. User A calculates **n_a = p_a * q_a = 143**. User A also calculates **phi_a = (p_a - 1) * (q_a - 1) = 120**. Then User A chooses a **e_a** number that is smaller than **phi_a** and relatively prime to **phi_a**, in this case **e_a = 119**. Finally, User A calculates **d_a** which is the inverse modulo **e_a** to **phi_a**. **(e_a, n_a)** is User A's public key and **(d_a, n_a)** is User A's private key. The same process is repeated by User B with different prime numbers, say **p_b = 17**, **q_b = 19**, resulting in a public key **(e_b, n_b) = (179, 323)** and a private **key (d_b, n_b)**.

RESULTS AND DISCUSSION

Problem Analysis

In the explanation above, by using cryptographic techniques in chat applications, encryption can be kept confidential so that not everyone can see the contents. Maintaining the confidentiality of messages is important because if the message is known by irresponsible parties, it will be misused, the company can suffer losses. Therefore, a chat app with data security is needed to protect data, and the right solution is to use *the Advanced Encryption Standard* (AES) cryptographic algorithm.

Database Design

Table 1. Name : Users

1.	id	int	11
2.	Powered by E-Mail	Varchar	50
3.	Lost your password?	Varchar	255
4.	profile_photo	Varchar	255
5.	Status		
6.	last_seen	Timestamp	

Source: Data Processed

Table 2. Table Name : Messages

1.	id	int	11
2.	user_id	int	11
3.	Message	Text	
4.	created_at	Timestamp	
5.	recipient_id	int	11
6.	Timestamp	Timestamp	
7.	file_path	Varchar	1500

Source: Data Processed

Application Flowchart

1. Here is the flowchart of the registration page

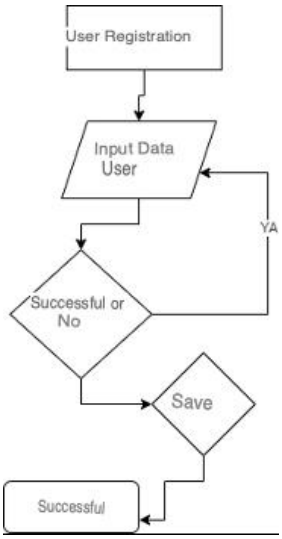

Figure 4. flowchart of the registration page

On the registration page where the user is required to input username, password and photo data and after that click on the registration page

2. Here is the flowchart flow of the application login page:

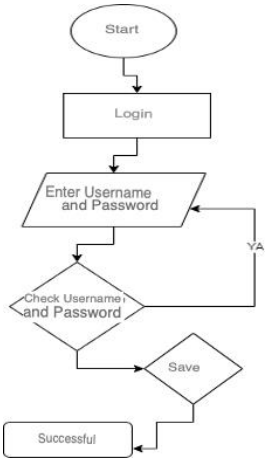

Figure 5. Flowchart Flow of the Application Login Page

On the login page where the user is required to input the username, password data and after that click on the page click the login button

3. Here is the flowchart of the home page:

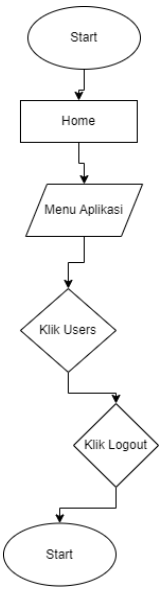

Figure 6. Flowchart of the home page

4. RSA encryption process flowchart and algorithm

   On the home page, there is a main menu on the application page, including the application, user and message menus.

Program Implementation

In the implementation stage, the system is made based on the design of the database and the appearance of the system in accordance with the system design. The implementation of the system that has been created is:

System Testing

1. Registration page

On the registration page, users are required to enter their username, e-email and password in order to log in and access the main page of the public complaint application.

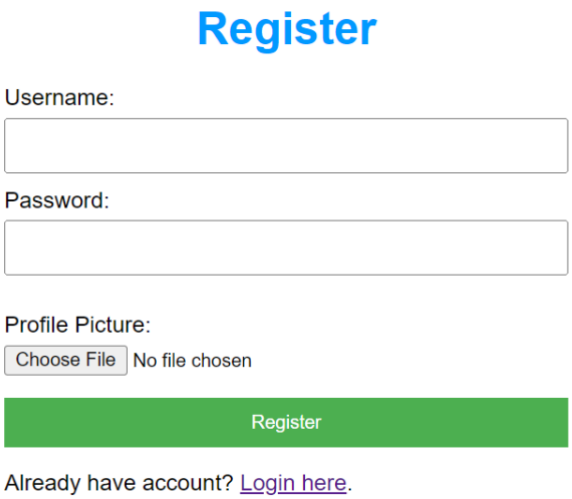

Figure 7. Register

2. Login Page

After registering, users are required to enter the email and password according to the registration form, after entering the email and password according to the registration form, click the login button, in order to access the dashboard page of the public complaint application.

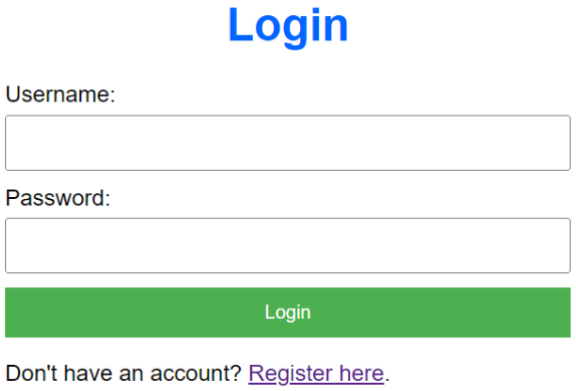

Figure 8. Login Page

3. Chat App Home Page

After successfully completing the login process, the user will switch to the home page. On the page, users can also chat where in this application the database is automatically encrypted the content of the message that the input is drawn several conclusions as follows.

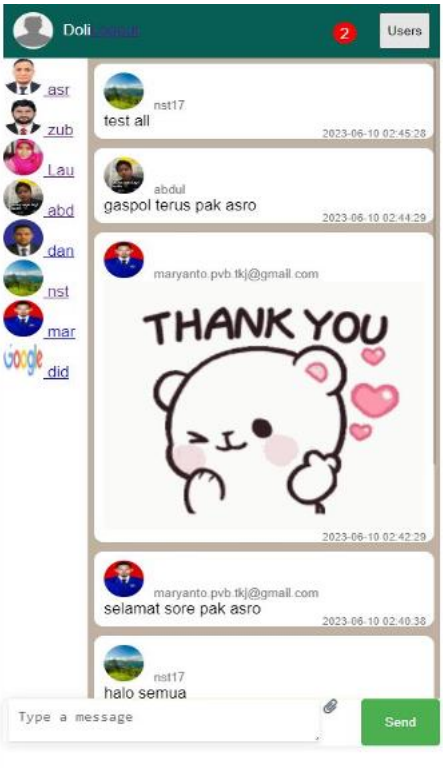

Figure 9. Chat App Home Page

CONCLUSION

The results of this study indicate that messages can be securely encrypted using the implemented method and stored within the database, as demonstrated by successful testing of message transmission and reception in the web-based chat application where all messages were effectively encrypted. Furthermore, the process of sending and receiving messages between mobile and web-based platforms operated smoothly, as evidenced by successful group chat functionality during testing. The application also proved capable of accurately decrypting encrypted messages sent from the sender's device, with all four test scenarios showing that the decrypted messages matched the original content. Additionally, the system requirements analysis revealed that the minimum browser versions required to run the web-based chat application are Google Chrome version 4x or higher and Mozilla Firefox version 3x or higher.

REFERENCE

Abudalou, M. (2024). Enhancing Data Security Through Advanced Cryptographic Techniques. *International Journal Of Computer Science And Mobile Computing*, *13*(1), 88–92. Https://Doi.Org/10.47760/Ijcsmc.2024.V13i01.007

Arief Prasada, D., Informasi, T., Luhur, U. B., Ciledug, J. R., Utara, P., & Selatan, J. (2018a). *Aplikasi Chatting Berbasis Web Dengan Algoritma Caesar Cipher Dan 3des Pada Cv. Felitechno Mandiri Untuk Pengamanan Pesan Pada Database* (Vol. 1, Number Maret).

Arief Prasada, D., Informasi, T., Luhur, U. B., Ciledug, J. R., Utara, P., & Selatan, J.

(2018b). *Aplikasi Chatting Berbasis Web Dengan Algoritma Caesar Cipher Dan 3des Pada Cv. Felitechno Mandiri Untuk Pengamanan Pesan Pada Database* (Vol. 1, Number Maret).

Badad Alauddin, M., Fitri, D., & Apri Wenando, F. (2025). Tradition To Technology: The Transformation Of Indonesian Culture In The Social Media Era. *Asian Journal Of Media And Culture*, *1*(1), 1–21. Https://Doi.Org/10.63919/Ajmc.V1i1.16

Beumier, C., & Debatty, T. (2022). Attack Detection In Ss7. *Communications In Computer And Information Science*, *1689 Ccis*. Https://Doi.Org/10.1007/978-3-031-20215-5_2

Bimantoro, Y., Titi, R., & Sari, K. (2021). Enkripsi Data Menggunakan Rsa & Aes Pada Aplikasi Instant Messaging Berbasis Mobile. *Jurnal Teknik Informatika*, *14*(2). Https://Doi.Org/10.15408/Jti.V14i2.23469

De Carvalho Macedo, L. O. H., & Campista, M. E. M. (2023). Attacks To Mobile Networks Using Ss7 Vulnerabilities: A Real Traffic Analysis. *Telecommunication Systems*, *83*(3). Https://Doi.Org/10.1007/S11235-023-01018-0

Dowling, B., Hale, B., Tian, X., & Wimalasiri, B. (2025). Cryptography Is Rocket Science. *Iacr Communications In Cryptology*, *1*(4). Https://Doi.Org/10.62056/A39qudhdj

Jensen, K., Van Do, T., Nguyen, H. T., & Arnes, A. (2016). Better Protection Of Ss7 Networks With Machine Learning. *2016 6th International Conference On It Convergence And Security, Icitcs 2016*. Https://Doi.Org/10.1109/Icitcs.2016.7740315

Khaziev, Sh. N., & Shtokhov, A. N. (2025). Cryptography In Forensic Science And Forensic Examination: History And Current State. *Theory And Practice Of Forensic Science*, *20*(2). Https://Doi.Org/10.30764/1819-2785-2025-2-6-21

Kılıç, M. B. (2021). Encryption Methods And Comparison Of Popular Chat Applications. *Advances In Artificial Intelligence Research*, *1*(2).

Kundiya, K. R. (2023). Enhanced Security Of Information By Integrating Steganography , Cryptography , And Genetic Algorithms. *International Research Journal Of Modernization In Engineering Technology And Science*, *05*(06).

Nasrullah, A. H. (2025). Secure Web-Based File Encryption Using Aes-128. *Journal Of Embedded Systems, Security And Intelligent Systems*, 146–155. Https://Doi.Org/10.59562/Jessi.V6i2.8436

Navid Bin Anwar, M., Hasan, M., Hasan, M., Loren, J. Z., & Tanjim Hossain, S. M. (2019). Comparative Study Of Cryptography Algorithms And Its' Applications. In *International Journal Of Computer Networks And Communications Security* (Vol. 7, Number 5).

Parmar, M., & Kaur, H. J. (2021). Comparative Analysis Of Secured Hash Algorithms For Blockchain Technology And Internet Of Things. *International Journal Of Advanced Computer Science And Applications*, *12*(3). Https://Doi.Org/10.14569/Ijacsa.2021.0120335

Prasetyo, R., & Suryana, A. (2016). Aplikasi Pengamanan Data Dengan Teknik

Algoritma Kriptografi Aes Dan Fungsi Hash Sha-1 Berbasis Desktop. In *Jurnal Sisfokom* (Vol. 05).

Prashant P. Pittalia. (2019). A Comparative Study Of Hash Algorithms In Cryptography. *International Journal Of Computer Science And Mobile Computing*, *8*(6).

Saeed, B. F., & Azadeh, I. R. (2024). When Cryptography Stops Data Science: Strategies For Resolving The Conflicts Between Data Scientists And Cryptographers. In *Data Science And Management* (Vol. 7, Number 3). Https://Doi.Org/10.1016/J.Dsm.2024.03.001

Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016a). Kriptografi Advanced Encryption Standard (Aes) Untuk Penyandian File Dokumen. *Jurnal Matematika Unisba*, *15*(1). Http://Ejournal.Unisba.Ac.Id

Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016b). Kriptografi Advanced Encryption Standard (Aes) Untuk Penyandian File Dokumen. *Jurnal Matematika Unisba*, *15*(1). Http://Ejournal.Unisba.Ac.Id

Ullah, K., Rashid, I., Afzal, H., Iqbal, M. M. W., Bangash, Y. A., & Abbas, H. (2020). Ss7 Vulnerabilities - A Survey And Implementation Of Machine Learning Vs Rule Based Filtering For Detection Of Ss7 Network Attacks. *Ieee Communications Surveys And Tutorials*, *22*(2). Https://Doi.Org/10.1109/Comst.2020.2971757