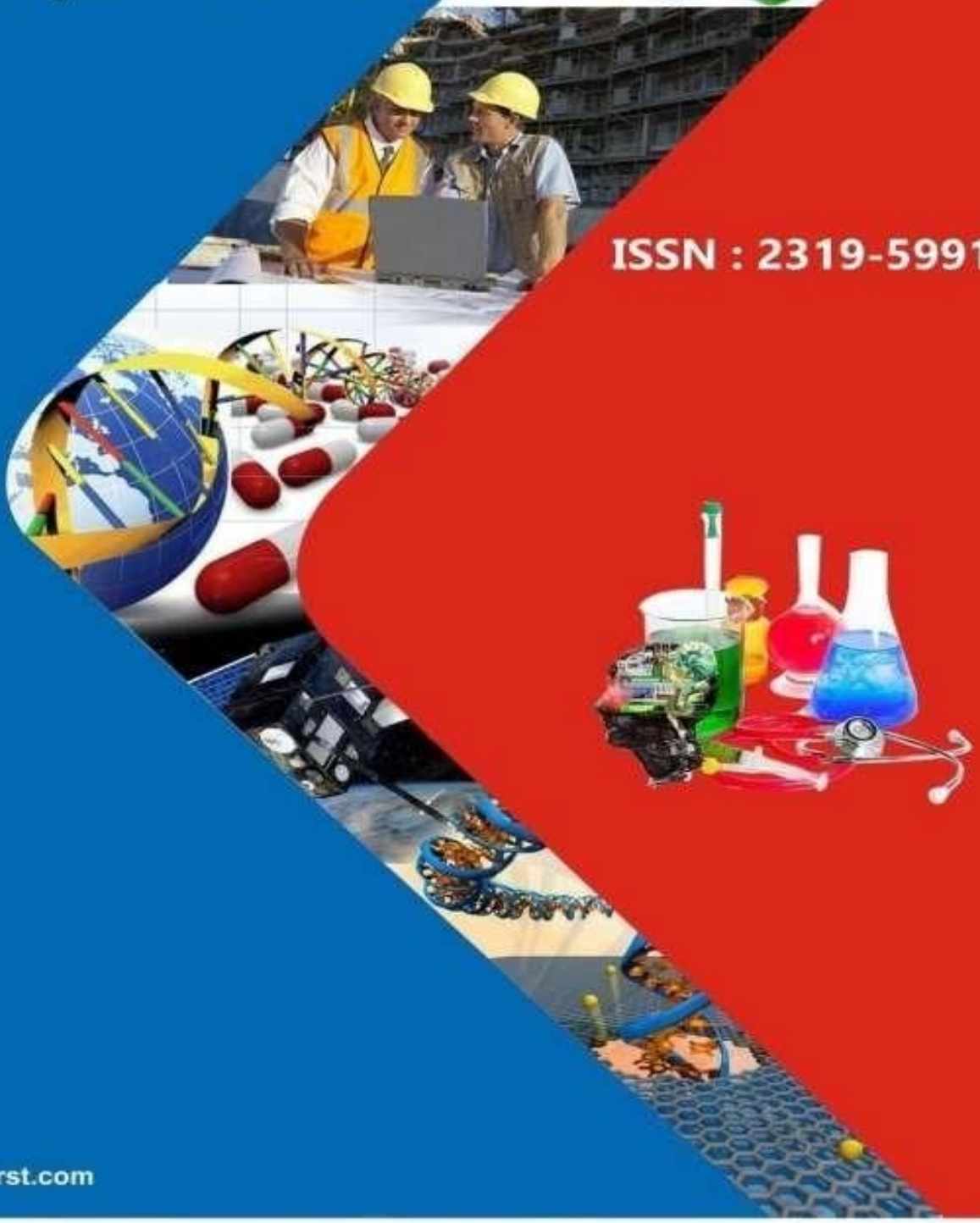
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

SMS ENCRYPTION SYSTEM

[1]KADIYAM SOMASEKHAR

[2]S.K.Alisha

B.V. Raju College, Vishnupur, Bhimavaram

ADIKAVI NANNAYA UNIVERSITY RAJAHMAHENDRAVARAM

I. INTRODUCTION

Nowadays, SMS is more and more common among mobile phone users. SMS is a text messaging service component of mobile phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices. Users can used SMS to send or receive from a single person, or several persons, personal messages, email notifications, information services, school activity alerts, notification from teacher, job dispatches, and also stock alerts. However, the security issue of SMS's is still an open challenging task. SMS is now a very common communication tool. The security protection of SMS messages is not yet that sophisticated and difficult to implement in practice. The confidentiality and integrity mechanisms are only specified as optional security measures that can be made available, but they are not mandatory requirements for SMS system implementation. In this paper, we have implemented three of block cipher symmetric cryptography algorithms (i.e. AES algorithm, DES, and 3-DES) and compared between three of them in terms of encryption and decryption delay time. This provides a guideline for the choice of the most suitable cryptography algorithm for mobile communication on Android message application.

II. LITERATURE SURVEY

SMS Vulnerabilities and the Need for Encryption

AUTHORS: Kharrazi. M, Khresheh. N.

Introduction to SMS and its Security Risks Short Message Service (SMS) has become an integral part of mobile communication, allowing users to exchange text messages over cellular networks. Despite its popularity, SMS does not provide any inherent security, making it vulnerable to various attacks such as eavesdropping, message tampering, and unauthorized access. As a result, ensuring the confidentiality, integrity, and authenticity of SMS messages is a crucial concern for secure mobile communication.

AES, DES, 3DES Enhanced security with

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

performance cost

AUTHORS: Deamen. J, Rijmen. V.

AES (Advanced Encryption Standard) AES is a widely accepted symmetric encryption algorithm, known for its security and efficiency. It operates on fixed-size blocks of data (128 bits) and supports key sizes of 128, 192, and 256 bits. AES is considered highly secure and is the standard for many applications, including secure messaging. Studies have shown that AES provides strong encryption and decryption security with relatively low computational overhead, making it suitable for mobile applications where both security and performance are essential.

DES (Data Encryption Standard) DES is one of the oldest symmetric encryption algorithms, developed in the 1970s, and was widely used in early cryptographic systems. However, due to advances in computational power, DES is now considered insecure for many applications, as its 56-bit key size can be easily cracked by modern brute-force attacks. Despite its weaknesses, DES is still relevant for comparative analysis in encryption performance studies.

3DES (Triple DES) 3DES is a modification of DES, designed to overcome the weaknesses of the original DES algorithm. It applies the DES algorithm three times with different keys, increasing the key length to 168 bits. Although 3DES provides a higher level of security than DES, it is less efficient than AES due to its multiple encryption steps, which can lead to slower performance, especially on mobile devices with limited processing power.

Comparative Studies on Symmetric Encryption for SMS

AUTHORS: Ajay Shankar Singh & S. B. Singh

Comparative Analysis of AES, DES, and 3DES Various studies have compared the performance of AES, DES, and 3DES in the context of mobile communication, specifically SMS encryption. The main criteria for comparison are encryption/decryption delay time, memory usage, and security strength. AES typically outperforms DES and 3DES in terms of encryption speed and security, making it the preferred choice for many mobile applications. 3DES, while more secure than DES, suffers from performance limitations due to its triple encryption process. In contrast, AES provides a good balance between security and performance, making it ideal for mobile platforms.

Implementation and Performance of using Algorithms

AUTHORS :Dr. Shubham Pawar

SMS Encryption Implementation and Performance Several research papers have proposed methods for implementing SMS

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

encryption using AES, DES, and 3DES. These studies typically evaluate the encryption and decryption delay times as a performance metric. In most cases, AES outperforms both DES and 3DES in terms of speed while maintaining a high level of security. However, the choice of algorithm may depend on the specific requirements of the mobile application, such as the trade-off between speed and the level of security needed.

Security Analysis and Conclusion

AUTHORS: Patil. A. M, Dinesha H A, Dr. V. Kiran kumar

Conclusion and Future Directions Based on the comparative studies, AES is generally the most suitable algorithm for SMS encryption in modern mobile communication due to its security strength and efficient performance. However, there is ongoing research aimed at improving the efficiency of cryptographic algorithms in mobile devices, including hardware acceleration and algorithm optimization.

Future studies may also explore hybrid approaches, combining multiple algorithms to enhance both security and performance. The implementation of AES, DES, and 3DES for SMS encryption systems has been widely studied, with AES consistently outperforming DES and 3DES in terms of encryption speed and security. AES is favored for modern mobile communication due to its efficient performance, low computational overhead, and high security. 3DES, while more secure than DES, suffers from slower performance, making it less suitable for SMS encryption in resource-constrained mobile devices. Thus, AES remains the most practical choice for SMS encryption in mobile applications.

III. PROBLEM STATEMENT

Existing SMS encryption systems primarily rely on end-to-end encryption (E2EE) and cryptographic protocols to secure text messages from unauthorized access. Traditional SMS lacks built-in encryption, making it vulnerable to interception by attackers or network providers. To address this, applications like Signal, WhatsApp, and Telegram use strong encryption algorithms such as AES, RSA, and Signal Protocol to ensure only the intended recipient can read the messages. Some systems implement public-key cryptography, where messages are encrypted with the recipient's public key and decrypted using their private key. However, standard SMS services provided by carriers do not support such encryption, leaving messages exposed to risks like man-in-the-middle attacks and surveillance.

3.1 DISADVANTAGES OF EXISTING SYSTEM

Existing SMS encryption systems have several disadvantages, primarily due to the

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

lack of native encryption in traditional SMS protocols. Since standard SMS relies on cellular networks, messages can be intercepted by attackers, network providers, or government agencies. Encrypted messaging apps offer security but require both sender and receiver to use the same platform, limiting interoperability. Additionally, encryption adds computational overhead, which may affect performance on low-end devices. Some encryption methods rely on internet connectivity, making them ineffective for offline SMS communication. Furthermore, key management in public-key encryption systems can be complex, and users who lose access to their private keys may be unable to decrypt past messages.

IV. PROPOSED SYSTEM

The proposed SMS encryption system aims to enhance security by integrating end to-end encryption (E2EE) into traditional SMS communication without relying on third-party messaging apps. It employs a hybrid cryptographic approach using AES for fast symmetric encryption and RSA for secure key exchange. Each user will have a unique public-private key pair, allowing messages to be encrypted with the recipient's public key and decrypted with their private key. A secure key exchange mechanism, such as Diffie-Hellman, ensures that only authorized users can access the encryption keys. The system will also include message integrity checks using hashing algorithms like SHA-256 to prevent tampering. Unlike existing solutions, this system will work over regular SMS networks, ensuring confidentiality even when no internet connection is available.

4.1ADVANTAGES OF PROPOSED SYSTEM

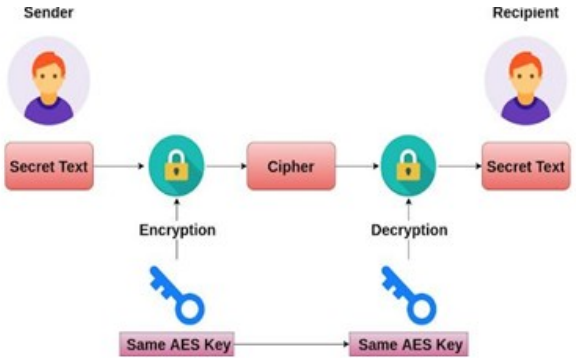
The proposed SMS encryption system offers several advantages over traditional SMS and existing encrypted messaging apps. By integrating end-to-end encryption (E2EE) into standard SMS, it ensures that only the intended recipient can read messages, protecting against interception by attackers, network providers, or government agencies. The use of a hybrid cryptographic approach (AES for fast encryption and RSA for secure key exchange) enhances both security and efficiency. Unlike internet-dependent messaging apps, this system works over regular cellular networks, making it accessible even in areas with limited or no internet connectivity. Additionally, message integrity verification using SHA-256 prevents tampering and ensures authenticity. The system's user-friendly key management reduces complexity, providing strong security without requiring advanced technical knowledge from users.

Algorithms: Advanced Encryption Standard, Data Encryption Standard,

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

Triple DES.

V. SYSTEM ARCHITECTURE



System Architecture

VI. SYSTEM IMPLEMENTATION

6.1 User

The **User Module** is a core component of the SMS Encryption System that facilitates interaction between the user and the application. It provides the necessary interface for users to compose, send, receive, and view SMS messages securely. This module allows users to input message content, choose the desired encryption algorithm (AES, DES, or 3DES), and initiate the encryption process before sending messages. Upon receiving messages, the module also provides options to decrypt and display the original plaintext using the correct decryption key.

The User Module is tightly integrated with the Authentication Module to ensure that all functionalities are only accessible to authorized users. It also communicates with the Encryption and Decryption Modules to perform cryptographic operations seamlessly in the background. Additionally, it provides basic user settings and profile management options, enhancing the overall usability and personalization of the application.

This module is designed to be user-friendly and intuitive, aiming to ensure a secure and efficient communication experience while maintaining the confidentiality and integrity of sensitive information transmitted via SMS.

6.2 Encryption Module

The **Encryption Module** is the core security component of the SMS Encryption System, designed to ensure the confidentiality of messages during transmission. Once a message is composed and validated through the Message Composition & Input Module, it is passed to this module for encryption. The module supports multiple symmetric block cipher algorithms, specifically **AES**, **DES**, and **3DES**, allowing users or the system to choose the appropriate algorithm based on security requirements or performance considerations.

6.3 Decryption Module:

The Decryption Module is responsible for converting encrypted SMS messages (ciphertext) back into their original readable form (plaintext). This module activates

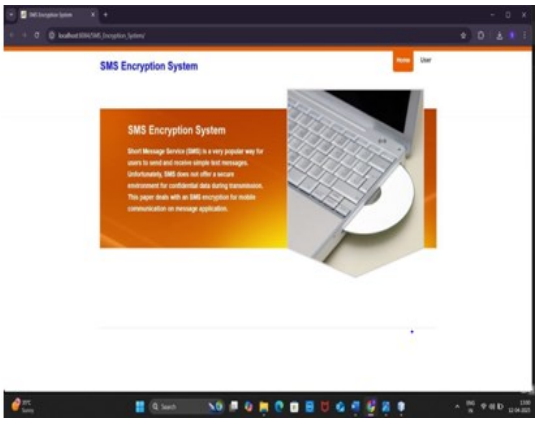
International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

when a user receives a message and provides the correct decryption key. It supports the same symmetric encryption algorithms implemented in the Encryption Module — AES, DES, and 3DES — ensuring compatibility and secure communication between users.

Upon receiving the encrypted message from the Message Transmission Module, the ecryption Module identifies the algorithm used and applies the corresponding decryption process using the associated secret key. It performs key validation and error checking to ensure that the message has not been altered or corrupted during transmission. If the key is incorrect or the message integrity is compromised, appropriate error messages are displayed to the user.

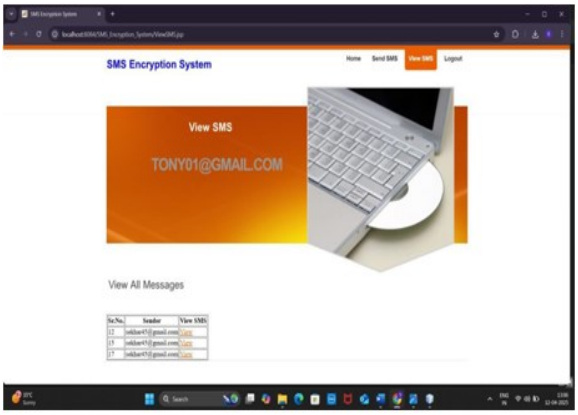
VII. RESULT ANALYSIS

HOME PAGE:



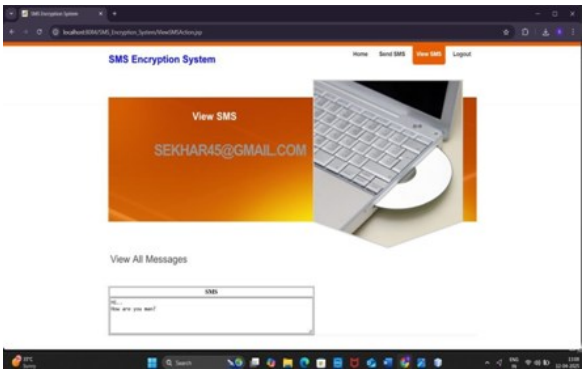
Home page.

VIEW SMS PAGE



View SMS page

USER VIEW SMS PAGE:



User View SMS Page

VIII. CONCLUSION

Using SMS for communication and information exchange, care should be taken when sensitive information is transmitted using SMS through unsecure channel. The users should be aware that SMS messages might be subject to interception from un-authorized access. In this paper, the application of SMS encryption for some of block cipher cryptographic encryption algorithms (i.e. AES, DES, 3-DES) on android application has been designed and

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

implemented. The SMS encryption application is running in the mobile phone or web which does not require any additional encryption devices.

IX. FUTURE WORK

In future enhancements of the SMS Encryption System, a primary focus could be the integration of more advanced and efficient cryptographic algorithms tailored for mobile environments. While the current implementation compares AES, DES, and 3DES, there is scope to evaluate newer lightweight cryptographic algorithms such as Blowfish, Two fish, and ChaCha20, which offer strong security with lower computational overhead. These algorithms are particularly suitable for devices with limited processing power and memory, ensuring minimal impact on performance during encryption and decryption. Furthermore, the introduction of hybrid encryption methods—combining symmetric and asymmetric techniques—can provide an additional layer of security, especially during key exchange processes. Implementing secure key management systems using Elliptic Curve Cryptography (ECC) or RSA could address vulnerabilities associated with symmetric key distribution.

Another important area for future work involves enhancing the user experience and broadening the application's capabilities beyond SMS. A mobile application with a well- designed user interface can be developed to support encrypted communication not only through SMS but also through other messaging platforms such as WhatsApp, Signal, or email. The integration of features such as secure message archiving, encrypted backups, and cloud synchronization would greatly benefit users who require reliable and secure communication tools. Additionally, adding biometric or multi-factor authentication mechanisms can increase the security level by ensuring only authorized users can access the encrypted messages. Real-time alerts and monitoring for suspicious activities or unauthorized access attempts could also be incorporated to bolster security further.

Lastly, future work can focus on testing and validating the SMS Encryption System in real-world environments to assess its performance under different network conditions and on various mobile devices. Extensive benchmarking across diverse hardware and operating systems (like Android and iOS) can help identify potential bottlenecks and optimize the encryption-decryption process. Scalability and interoperability tests should also be conducted to ensure that the system works seamlessly with existing mobile infrastructure and SMS gateways. In addition, incorporating compliance with legal and regulatory standards such as

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

GDPR or HIPAA could make the system viable for use in sensitive sectors like healthcare, finance, and government communications. By addressing these aspects, the system can evolve into a robust, secure, and practical solution for mobile communication.

BIBILIOGRAPHY

1.1 REFERENCES

[1] Harb, Hany, Hassan Farahat, and Mohamed Ezz. "SecureSMSPay: secure SMS mobile payment model." In Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference on, pp. 11-17. IEEE, 2008.

[2] Lisoněk, David, and Martin Drahansky. "Sms encryption for mobile communication." In Security Technology, 2008. SECTECH'08. International Conference on, pp. 198-201. IEEE, 2008.

[3] Rayarikar, Rohan, Sanket Upadhyay, and Priyanka Pimpale. "SMS Encryption using AES Algorithm on Android." International Journal of Computer Applications 50, no. 19 (2012).

[4] Ariffi, Suriyani, Ramlan Mahmod, Ratini Rahmat, and Nuzul Annisa Idris. "SMS Encryption Using 3DAES Block Cipher on Android Message Application." In Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on, pp. 310-314. IEEE, 2013.

[5] Hassinen, Marko. "SafeSMS-end-to-end encryption for SMS." InTelecommunications, 2005. ConTEL 2005. Proceedings of the 8th International Conference on, vol. 2, pp. 359-365. IEEE, 2005.