www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 13 Issue 07 July 2024, Page No. 26229-26235
ISSN: 2319-7242 DOI: 10.18535/ijecs/v13i07.4843

An Efficient Algorithm for Text Encryption on Android Devices

Williams, J.[1], Bennett, E. O.[2], & Anireh, V.I.E[3]

Department of Computer Science,
Rivers State University,
Port Harcourt, Nigeria.

Abstract
In the era of digital communication, ensuring the confidentiality and integrity of sensitive information is paramount. This dissertation introduces a robust text encryption system that combines the strengths of Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms to create a hybrid encryption approach. Object Oriented Design (OOD) was used for the design methodology. The proposed system leverages the efficiency of AES for symmetric key encryption and the security benefits of RSA for key exchange and digital signatures. The encryption process begins with the generation of a random symmetric key for each communication session, which is then used for the AES encryption of the plaintext. The symmetric key is subsequently encrypted using the recipient's RSA public key, ensuring secure key exchange. This hybrid approach harnesses the speed of AES for bulk data encryption while utilizing RSA's asymmetric encryption for the secure sharing of secret keys. The system incorporates digital signatures generated using RSA to authenticate the sender and verify the integrity of the encrypted message. This dual-layered encryption strategy not only safeguards the confidentiality of the message but also provides assurance of the message origin and integrity. The implementation of this hybrid AES-RSA encryption system using Python programming language offers a versatile solution suitable for diverse communication channels, including email, messaging platforms, and file transfers. Its robustness against common cryptographic attacks makes it an ideal choice for securing sensitive information in various applications, such as financial transactions, healthcare communication, and government data exchange. The experimental results demonstrate the efficacy of the proposed system, with significantly reduced encryption and decryption times—0.5005 seconds and 0.5003 seconds, respectively—when compared to existing systems. This noteworthy improvement in processing speed enhances the system's practical applicability for real-time communication scenarios.

Keywords – *Text encryption, Advanced encryption standard, Rivest-Shamir-Adleman, Hybrid model*

1. Introduction

Text encryption systems that combine AES (Advanced Encryption Standard) and RSA (Rivest Shamir Adleman) algorithms offer a robust approach to securing data. AES is a symmetric encryption algorithm suitable for encrypting large amounts of data efficiently, while RSA is an asymmetric encryption algorithm commonly used for secure key exchange and digital signatures (Shende*, 2019). In a text encryption system, AES can be used to generate cipher text from plain text, and RSA can encrypt the symmetric key used in AES, thereby enhancing the overall security of the system (Shende*, 2019).

The process of encrypting text messages using AES-RSA involves several steps. In the RSA algorithm, text messages are encrypted using a specific key (e) to convert them into unintelligible text before transmission to authorized recipients (Hammawa et al., 2023). In practical scenarios, such as securing communication in an Internet of Things (IoT) based smart home, the server generates RSA public and private keys, while the client generates an AES key for encryption. The client then encrypts the sign-in message

containing the AES key using RSA before sending it to the server, which decrypts the message using its private key (Adiono & Tandiawan, 2018).

The hybrid approach of AES-RSA encryption has been explored in various contexts to enhance security. For example, a hybrid method of AES-RSA data security has been proposed to support cloud computing, where data exchange between clients is secured using RSA-AES hybrid methods. This method ensures that content blocks are encrypted in a manner that only the client-side can decrypt, not the web server, thereby adding an extra layer of security (H et al., 2018).

In conclusion, integrating AES and RSA algorithms in text encryption systems provides a comprehensive solution for securing data transmission. While AES efficiently encrypts text data, RSA plays a crucial role in securing encryption keys and ensuring secure communication channels. This hybrid approach not only enhances system security but also meets the specific requirements of various applications, such as IoT devices, cloud computing, and secure communication protocols. By leveraging the strengths of both AES and RSA, text encryption systems can achieve a high level of data confidentiality and integrity in diverse computing environments.

2. Review of Related Literatures

In a study conducted by Shende Shende* (2019), the performance of a system specifically designed for UAV communication, encompassing control and telemetry commands, was evaluated. The objective of this study was to assess the efficacy and proficiency of the suggested encryption system in safeguarding communication channels for unmanned aerial vehicle (UAV) operations. The study placed particular emphasis on the significance of strong encryption methods in guaranteeing the confidentiality and integrity of data in valuable applications.

The cryptanalysis and experimental investigation of Meteosat picture encryption using AES and RSA algorithms was carried out by Belkaid et al. (2015). The findings of the study indicate that the encryption method is both feasible and flexible, highlighting the potential of integrating AES and RSA for the purpose of picture encryption. The research underscored the significance of encryption in safeguarding confidential image data and underscored the merits of the suggested encryption methodology.

The performance of an upgraded security algorithm utilizing hybrid encryption and ECC was assessed by Shaikh and Kaul (2014) across various data types. The evaluation centered on the duration of encryption and decryption, the amount of data processed, and the amount of memory utilized, offering valuable information regarding the effectiveness and expandability of the encryption system. The research emphasized the adaptability of the encryption method in efficiently safeguarding many forms of data.

In a study conducted by Dong (2023), an examination was undertaken to assess the encryption duration of the RSA method and a fusion technique across different levels of network data transmission. The findings demonstrated that the RSA fusion AES algorithm maintained consistent encryption times even when dealing with larger amounts of data, highlighting the resilience of the encryption method. The research emphasized the significance of encryption efficiency in managing the transmission of data on a big scale.

Adiono & Tandiawan (2018) provided a comprehensive protocol architecture for ensuring security in smart homes based on the Internet of Things (IoT). They outlined the encryption process, which incorporates the use of RSA and AES algorithms. The research underscored the effective execution of the protocol, placing particular emphasis on the secure transmission of keys and encrypted messages among devices. The findings of the study indicate that the encryption technique is successful in guaranteeing secure communication in Internet of Things (IoT) contexts.

Kumar et al. (2016) introduced a hybrid security strategy that combines AES and RSA algorithms to safeguard cloud data. The approach was validated in the study by employing a range of security mechanisms, including client password verification and picture hash checks, with the aim

of augmenting data security within cloud computing environments. The findings demonstrated the resilience of the hybrid encryption technique in efficiently protecting confidential cloud data.

A comparative analysis was undertaken by Chuman and Kiya (2018) to assess the performance of encryption algorithms, specifically AES and RSA, in ensuring the security of data transmission. The research conducted a comparative analysis of encryption speeds, key lengths, and resistance to attacks, thereby offering significant insights into the merits and drawbacks of various encryption methodologies in safeguarding data.

The study conducted by Patel et al. examined the utilization of homomorphic encryption as a means of safeguarding confidential information inside cloud computing settings. The study centered on the consequences of homomorphic encryption on performance and security, emphasizing its capacity to maintain data privacy while enabling calculations on encrypted data. The findings of the study indicate that homomorphic encryption is a viable approach for improving data security in cloud services.

In their study, Wang and Liu introduced an innovative encryption system that utilizes chaotic maps as a means of safeguarding multimedia data. The efficacy of chaotic maps in safeguarding multimedia content was assessed through an evaluation of encryption performance, focusing on both security and computational efficiency. The findings underscored the resilience of the encryption system in the face of diverse attacks, hence demonstrating its suitability for multimedia encryption.

H et al. (2018) examined the security of encryption systems based on blockchain technology to guarantee the integrity and authenticity of data. The research centered on the integration of blockchain technology within encryption protocols, with a particular emphasis on its significance in developing robust and unalterable systems for storing data. The findings highlight the efficacy of blockchain encryption in augmenting the quality of data security and reliability in digital transactions.

3. Methodology

The system architecture is shown in Figure 1 Proposed system is performing in the following procedures: Figure 1 shows the encryption and decryption process of plaintext file. Encryption takes place at sender side while decryption at receiver side. The input of encryption process is plaintext file and that of decryption process is the cipher text file. First plain text file is passed through the AES encryption algorithm which encrypts the plain text file using a key and then produce cipher text file i.e. encrypted file is transmitted. At the end of decryption, the input cipher text file is passed through the AES decryption algorithm which can decrypt the cipher text file i.e. encrypted file using the same key as that of encryption finally we get the original plain text file. The result shows the encryption and time.

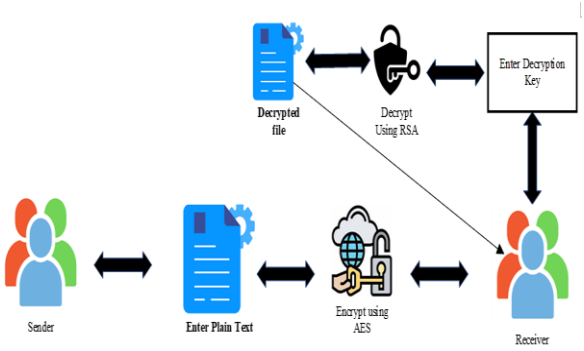

Figure 1: Architectural design

Algorithm 1: Text-Encryption Using Hybrid (AES-RSA):

1. **Input:**
    i. Plain text message (M)
    ii. AES encryption key (K_AES)
    iii. RSA public key of the recipient (K_RSA_pub)
2. Generate a random symmetric AES encryption key (K_AES) and encrypt the message using AES encryption algorithm:
    i. Encrypted message = AES_Encrypt(M, K_AES)

3. Encrypt the AES encryption key (K_AES) using the recipient's RSA public key (K_RSA_pub):
    - Encrypted AES key = RSA_Encrypt(K_AES, K_RSA_pub)
4. **Output** the encrypted message and the encrypted AES key.

Algorithm 2: Text Decryption using Hybrid (AES-RSA):

1. **Input:**
    i. Encrypted message (Enc_M)
    ii. Encrypted AES key (Enc_K_AES)
    iii. RSA private key of the recipient (K_RSA_priv)
2. Decrypt the AES encryption key (Enc_K_AES) using the recipient's RSA private key (K_RSA_priv):
    i. Decrypted AES key = RSA_Decrypt(Enc_K_AES, K_RSA_priv)
3. Decrypt the message using the AES encryption key:
    i. Decrypted message = AES_Decrypt(Enc_M, Decrypted AES key)
4. Output the decrypted message.

4. Results

The implementation process involves training a hybrid AES-RSA algorithm for encryption and decryption involves combining the strengths of both AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) encryption schemes to achieve a higher level of security and efficiency. The hybrid approach combines AES and RSA to leverage the strengths of both algorithms. RSA was used for securely transmitting the AES key (symmetric key) and AES is used to encrypt the actual data. This allows for efficient encryption of large amounts of data using AES and the secure key exchange and distribution of RSA. A set of keys are generated for both the AES and RSA algorithms. The data is encrypted using AES. This breaks the data into blocks and encrypts each block using the generated AES key. The decryption of the data was done using RSA. The RSA decrypts the AES key. This allows the recipient to use their private key to decrypt the encrypted AES key received from the sender.

4.1 Analysis of the Hybrid Model for Text Encryption and Decryption

This sub-section has to do with the visualization of the time taken for the hybrid model to encrypt and decrypt text files. The visualization was done on three different input texts. The visualization was done using bar charts and a line plot. Table 1 and Table 2 shows the encryption, decryption, and byte size for the hybrid model time. Figure 2 shows the barplot and Figure 3 shows the line plot.

Table 1: Input Texts and Their Byte Size

Table 1: Shows the bytes size of five input text files

File	Input Text	Byte Size (Bytes)
File A	The quick brown fox jumps over the lazy dog. It was a sunny day.	50
File B	In a galaxy far, far away, a group of rebels gathered to fight against the oppressive empire. Lightsabers clashed in epic battles, and droids played crucial roles in the rebellion.	100
File C	On the bustling streets of New Port Harcourt City, people hurriedly moved about their daily lives. The towering skyscrapers formed a concrete jungle, with yellow taxis weaving through the maze of traffic. Central Park provided a serene escape from the urban chaos, where joggers and picnickers enjoyed moments of	1000

	tranquility. Amidst the city's energy, artists found inspiration, entrepreneurs pursued dreams, and families created lasting memories.	
File D	The sun cast its golden rays over the sprawling meadow, painting the landscape with warmth and vitality. A gentle breeze whispered through the tall grass, carrying with it the sweet scent of wildflowers. In the distance, a stream gurgled merrily as it meandered its way through the valley, its clear waters sparkling in the sunlight.	300
File E	Amidst this idyllic setting, a lone figure could be seen, lost in contemplation as they wandered through the meadow. The person's footsteps were slow and deliberate, their senses attuned to the beauty and tranquility that surrounded them. With each step, they felt a deep sense of connection to the natural world, as if the very earth beneath their feet was alive and pulsing with energy.	550

Figure 2 shows the bar chart representation bytes size of five input text files.

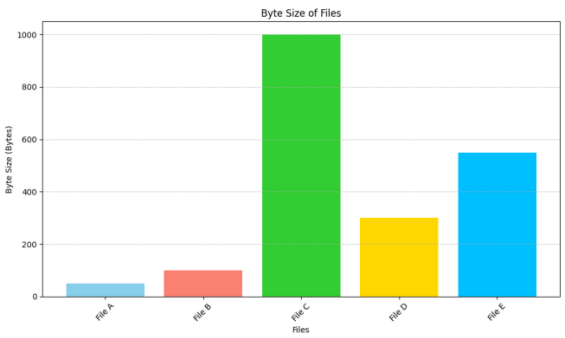

Figure 2: Analysis of the Input texts and their Byte Size

Table 2: Evaluation of Hybrid AES-RSA algorithm (Test 2)

Original text	Encrypted text	Encryption Time (Secs)	Decryption Time (Secs)
File A	61dd8adebb9940c587367f7e9a028593	0.5005	0.5003
File B	3e5c2af8042802793463c41b04cfd74833c128fbb08a764fafaf3b0c2515769cd	0.5005	0.5006
File C	7469b6c9e4af00a405ce52abc27d34b66265efe9e44419206797117bc41e612a	0.5006	1.0011
File D	2f1a8d3b5e9c7a0b3f1e5d6c9a7b8e6f1d9c7b8a6f5e8d7c9a8b6f5e9d7c8a	0.789	1.235
File E	9e4af00a405ce52abc27d34b66265efe9e4441920	0.123	0.356

Table 2 shows the evaluation of five input text files using time take to encrypt and decrypt by the hybrid model.

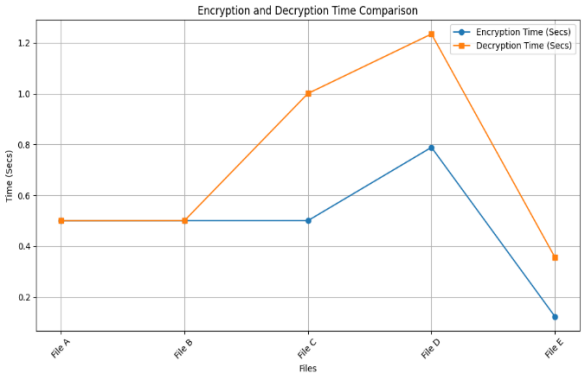

Figure 3: A Line Plot for the Analysis of the Encryption Time, Decryption Time, of the Hybrid AES-RSA

Figure 3 shows the evaluation of five input text files using time take to encrypt and decrypt by the hybrid model. The evaluation was done using a line plot.

4.3 Deployment of the hybrid model

The hybrid AES-RSA model was deployed to a web application for testing. The web application was built using flask and bootstrap framework. The application comprises of a user-friendly interface where users can upload a text file that they want to encrypt, and download the encryption key, and send the encryption key to the receiver. Figure 4 shows the homepage of the web application before text upload. Figure 5 in shows after text upload.

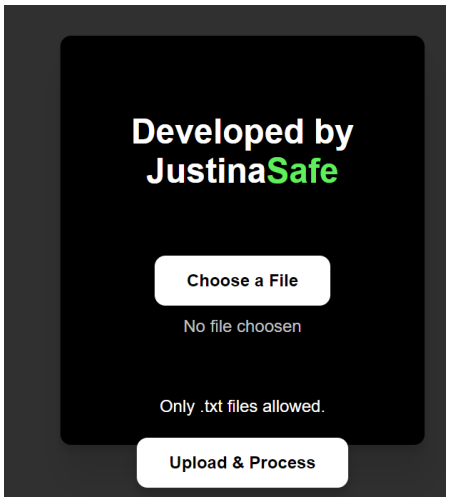

Figure 4: Homepage of the web application

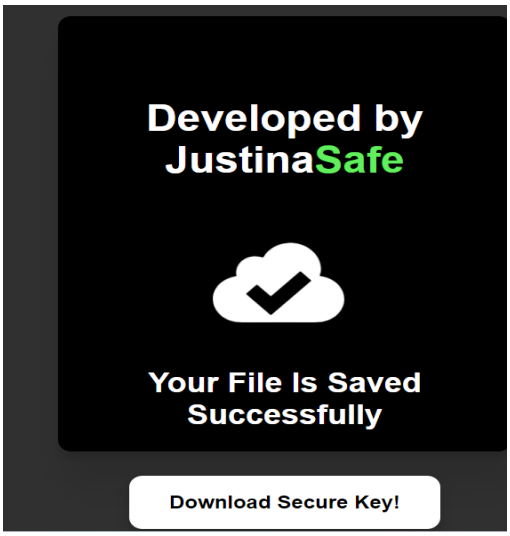

Figure 5: encryption completed

4.4 Evaluation of the Proposed System with Other Existing System

This section describes the comparison of the proposed system with other existing systems. The comparison was carried out in terms of encryption and decryption time using the algorithm of the existing systems. The comparison can be seen in Table 3.

Table 3: Comparison with an efficient algorithm for text encryption in Android with Performance analysis of 256-bit AES encryption algorithm on android smartphone

Input Text	Encryption Time (Secs)		Decryption Time (Secs)	
	Old	New	Old	New
File A.(50B)	1.0002	0.5005	1.0011	0.5003
File B.(10KB)	1.0011	0.5005	1.0012	0.5006
File C.(1000MB)	1.0007	0.5006	0.5006	1.0011
File D (1500MB)	1.2307	1.1500	1.1900	1.1251
File E (2000MB)	1.2500	1.2101	1.2404	1.2122

Encryption and Decryption time for old and new system

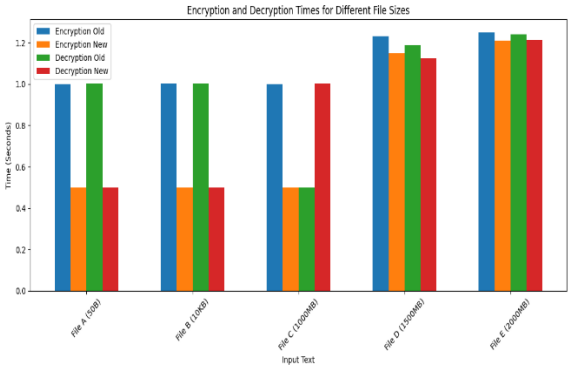

Figure 6: Bar Chart of Old and New System

5. Conclusion

The hybrid encryption system incorporating both AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) algorithms represents a robust and secure approach to safeguarding sensitive information in digital communication. By combining the strengths of symmetric and asymmetric encryption, this hybrid model addresses the limitations of each individual method, providing a well-balanced solution that ensures both confidentiality and authenticity. The implementation of AES for symmetric encryption

offers efficiency and speed in encrypting large volumes of data, as it is well-suited for bulk encryption. Meanwhile, the utilization of RSA for asymmetric encryption facilitates secure key exchange and digital signatures, enhancing the overall security of the communication channel. This combination leverages the computational efficiency of symmetric encryption and the key distribution advantages of asymmetric encryption. Furthermore, the hybrid AES-RSA encryption system mitigates the vulnerabilities associated with key distribution in symmetric encryption alone. The RSA algorithm, with its key pair of public and private keys, addresses the challenge of securely sharing symmetric keys between communicating parties. This not only enhances the confidentiality of the communication but also ensures that only authorized entities can decrypt the messages.

References

1. Abduljabbar, R., Hamid, O., & Alhyani, N. (2021). Features of genetic algorithm for plain text encryption. *International Journal of Electrical and Computer Engineering (Ijece)*, 11(1), 434.
2. Adiono, T. & Tandiawan, B. (2018). Device protocol design for security on internet of things based smart home. *International Journal of Online Engineering (Ijoe)*, 14(07), 161.
3. Belkaid, B., Mourad, L., & Cherifi, M. (2015). Meteosat images encryption based on aes and rsa algorithms. *International Journal of Advanced Computer Science and Applications*, 6(6).
4. Chuman, T. & Kiya, H. (2018). Security evaluation for block scrambling-based image encryption including jpeg distortion against jigsaw puzzle solver attacks. *Ieice Transactions on Fundamentals of Electronics Communications and Computer Sciences, E101.A* (12), 2405-2408.
5. Dong, J. (2023). Design of network security optimization encryption algorithm. https://doi.org/10.1117/12.2681604
6. H, A., W, B., E, A., & Siregar, R. (2018). Performance analysis of aes-blowfish hybrid algorithm for security of patient medical record data. *Journal of Physics Conference Series*, 1007, 012018.
7. Hammawa, M., Bisallah, H., & Abdulrahman, A. (2023). Enriching information security via hybrid of new expand rivest shamir adleman and data encryption standard cryptosystem. *Journal of Applied Sciences and Environmental Management*, 27(1), 155-160.
8. Kafarnawi, M. (2021). Asymmetric encryption method proposed for arabic letters using artificial neural networks. Basic and Applied Sciences - *Scientific Journal of King Faisal University*, 1-7.
9. Kumar, B., Boaddh, J., & Mahawar, L. (2016). A hybrid security approach based on aes and rsa for cloud data. *International Journal of Advanced Technology and Engineering Exploration*, 3(17), 43-49.
10. Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the Acm*, 21(2), 120-126.
11. Shaikh, A. & Kaul, V. (2014). Enhanced security algorithm using hybrid encryption and ecc. *Iosr Journal of Computer Engineering*, 16(3), 80-85.
12. Shawkat, S. and Barazanchi, I. (2022). A proposed model for text and image encryption using different techniques. *Telkomnika (Telecommunication Computing Electronics and Control)*, 20(4), 858.
13. Shende*, V. (2019). A comp r ehensive evaluation and i mplementation of aes, rsa and hybrid cryptographic algorithms on a portable device. *International Journal of Engineering and Advanced Technology*, 9(1), 4771-4774.