WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Hybrid Cryptosystem for Securing Myanmar Text Using Symmetric and Asymmetric Algorithms with Blockchain

Yi Mon Thet, Nilar Aye[b], Zin Thu Thu Myint[b], Hay Man Oo[b]*

University of Computer Studies, Yangon, Myanmar
E-mail address: yimonthet@ucsy.edu.mm

ABSTRACT

The increasing reliance on digital communication in Myanmar necessitates robust mechanisms for securing Myanmar language text against unauthorized access and tampering. Unlike English, the Myanmar script contains 33 consonants, 12 vowels, and 4 medials, forming complex character combinations that pose challenges for conventional cryptographic methods. This paper proposes a hybrid cryptosystem that combines symmetric encryption (AES), asymmetric encryption (RSA), and blockchain technology to achieve confidentiality, integrity, and secure key distribution. AES provides fast and efficient encryption of Myanmar text at the block level, while RSA is used to securely encrypt the AES session key, solving the key distribution problem. To enhance integrity and tamper resistance, ciphertext blocks are stored in a blockchain-linked structure,where each block contains cryptographic hashes of its predecessor, making any unauthorized modification immediately detectable. The proposed system is implemented in Python with support for complete Myanmar character sets. Experimental results demonstrate that the hybrid cryptosystem achieves low encryption and decryption time, robust security against brute-force attacks, and resistance to ciphertext tampering through blockchain verification. This work contributes a practical and language-awarecryptographic framework for the secure transmission of Myanmar text in e-government, financial, and communication applications.

Keywords: Myanmar Language Cryptography, AES, RSA, Blockchain, Hybrid Cryptosystem

1. Introduction

In recent years, the rapid expansion of digital communication in Myanmar has led to an increasing demand for secure transmission of textual data in the Myanmar language. From online banking and government e-services to social media and private messaging, the protection of sensitive information has become a critical priority. Unlike English, Myanmar script consists of 33 consonants, 12 vowels, and 4 medials, along with unique diacritical marks and stacked characters. This creates a much larger character space and presents additional challenges in encryption, as standard cryptosystems often assume fixed-size alphabets like ASCII or English letters. Consequently, a language-aware approach is required to ensure that Myanmar text can be encrypted and decrypted accurately without data loss or misinterpretation. Classical cryptography methods, such as the Caesar cipher, Vigenère cipher, or even modern stream ciphers, are insufficient to withstand modern cryptanalysis when applied directly to Myanmar text. Symmetric key cryptography, particularly Advanced Encryption Standard (AES), provides a robust and efficient mechanism for encrypting large blocks of text. However, symmetric algorithms face the key distribution problem, where securely sharing the secret key with the recipient can be difficult in an open network environment. On the other hand, asymmetric algorithms such as Rivest-Shamir-Adleman (RSA) solve the key exchange problem by allowing the AES session key to be encrypted with the recipient's public key, thus combining the speed of AES with the secure key management of RSA in a hybrid cryptosystem. To further enhance security and data integrity, this research integrates blockchain technology into the cryptosystem. Blockchain provides a linked, tamper-evident structure where each encrypted block of Myanmar text is chained using cryptographic hashes. This ensures that any unauthorized modification to the ciphertext can be instantly detected, enhancing resistance to tampering and replay attacks. By combining AES for symmetric encryption, RSA for secure key distribution, and blockchain for ciphertext integrity, the proposed hybrid cryptosystem addresses the critical challenges in securing Myanmar language communication.

The main contributions of this research are as follows:

- Development of a hybrid AES+RSA+Blockchain cryptosystem specifically designed for Myanmar text.
- Design of encryption and decryption algorithms capable of handling Myanmar characters, consonant-vowel combinations, and diacritical marks.
- Integration of blockchain to provide immutable and verifiable ciphertext storage, ensuring data integrity against tampering.
- Experimental evaluation of the system's encryption and decryption speed, security robustness, and resistance to brute-force and modification attacks.

2. Related Work

Securing textual communication has been a longstanding focus of cryptographic research, with methods evolving from classical ciphers to modern hybrid systems (Stallings, 2023; Schneier, 2015). Myanmar language cryptography presents unique challenges due to its large and complex character set, which includes stacked consonants, medials, and diacritical marks (Htet and Aye, 2020).

Early research on Myanmar text encryption primarily adopted classical substitution and polyalphabetic techniques such as Beaufort ciphers and Vigenère-based approaches (Htet and Aye, 2020; Aung and Hla, 2021). Htet and Aye (2020) introduced an enhanced Beaufort cipher combined with stream ciphers for Myanmar text. While this approach increased encryption complexity, it remained susceptible to frequency analysis and brute-force attacks due to predictable key spaces and the absence of robust key management.

To address these limitations, Aung and Hla (2021) proposed a Vigenère-Affine hybrid cipher to strengthen Myanmar language encryption. Although this method improved resistance to basic cryptanalysis, it lacked secure key exchange and did not provide integrity verification during transmission. Furthermore, both methods primarily operated on Unicode code points, which caused normalization and character rendering issues during encryption and decryption..

In recent years, blockchain technology has emerged as a promising tool for data integrity and tamper resistance (Nakamoto, 2008; Zheng et al., 2017). Blockchain's immutable, hash-linked structure has been applied in cybersecurity to detect unauthorized modifications of encrypted data. Meanwhile, hybrid cryptosystems that combine symmetric and asymmetric algorithms have gained popularity for secure communication:

- AES (symmetric) provides fast and efficient block encryption for large text data (NIST, 2001),
- RSA (asymmetric) solves the key distribution problem by securely exchanging session keys (Rivest et al., 1978), and
- Blockchain integration adds tamper detection by linking ciphertext blocks with cryptographic hashes (Zheng et al., 2017).

However, existing works seldom integrate a full AES+RSA+Blockchain hybrid cryptosystem for Myanmar text encryption. Most prior approaches focus on symmetric-only schemes or lack an integrity verification mechanism. This research bridges that gap by combining the efficiency of AES, the secure key management of RSA, and the tamper resistance of blockchain, resulting in a comprehensive security framework tailored to Myanmar language communication.

Table 1- Comparison of Existing Cryptographic Methods for Myanmar Text Encryption

Method	Key Features	Integrity Check	Key Management	Limitation
Beaufort + Stream Cipher	Classical Myanmar cipher	No	Manual Key	Vulnerable to frequency attack
Vigenère-Affine	Polyalphabetic hybrid	No	Manual Key	No tamper detection
AES-only (Symmetric)	Fast block encryption	No	Insecure Key	Key exchange problem
Proposed AES+RSA+Blockchain	Confidentiality + Integrity + Secure key exchange	Yes	RSA-secure	Slight storage overhead

The above table summarizes and compares key cryptographic methods previously applied to Myanmar text encryption, highlighting their main features, integrity verification capabilities, key management schemes, and limitations. Classical approaches such as Beaufort combined with stream ciphers and the Vigenère-Affine hybrid cipher lack built-in integrity checks and rely on manual key management, making them vulnerable to common cryptanalysis attacks and key distribution challenges. Symmetric-only schemes like AES provide efficient encryption but often suffer from insecure key exchange and absence of tamper detection. The proposed hybrid AES+RSA+Blockchain system addresses these shortcomings by integrating confidentiality, integrity verification, and secure key management, albeit with slightadditional storage overhead. This comparative analysis underscores the advantages of the proposed method within the context of Myanmar language cryptography.

3. Proposed Hybrid Cryptosystem

This research proposes a hybrid cryptosystem that integrates symmetric encryption (AES), asymmetric encryption (RSA), and blockchain technology to secure Myanmar language text transmission with confidentiality, integrity, and efficient key management.

3.1 System Overview

The proposed system operates in three key phases:

- Language-aware Symmetric Encryption with AES: Myanmar text input is first preprocessed to handle its complex script structure, including consonants, vowels, medials, and diacritical marks. The plaintext is segmented into fixed-size blocks compatible with AES encryption. AES is then applied to encrypt each block efficiently, ensuring fast encryption/decryption suited for large texts.

- Secure Key Distribution with RSA: To solve the key distribution challenge inherent in symmetric encryption, the AES session key is encrypted using the recipient's RSA public key. This ensures only the intended recipient, possessing the corresponding RSA private key, can decrypt the AES key securely, preventing interception or unauthorized access during key exchange.
- Integrity Verification via Blockchain: The ciphertext blocks produced by AES encryption are stored sequentially in a blockchain-like data structure. Each ciphertext block is linked with the cryptographic hash of the previous block, creating an immutable chain that detects any unauthorized modifications or tampering. This tamper-evident blockchain ensures data integrity during storage and transmission.

3.2 Detailed System Architecture

- Preprocessing Module: Parses Myanmar Unicode text, accurately handling composite characters, stacked consonants, and medials to form encryption-ready blocks without data loss or misinterpretation..
- AES Encryption Module:Utilizes the AES algorithm in a secure mode (e.g., CBC or GCM) for encrypting Myanmar text blocks. This symmetric encryption provides fast and secure transformation of plaintext to ciphertext.
- RSA Key Management Module:Generates RSA public/private key pairs for communicating parties. The AES session key used in encryption is encrypted with the recipient's RSA public key, ensuring secure key exchange.
- Blockchain Construction Module:Each AES-encrypted ciphertext block is linked with the previous block's hash value to form a blockchain ledger. This ledger is maintained to provide immutable, verifiable ciphertext storage, enabling detection of tampering or replay attacks.
- Decryption Module:The recipient first decrypts the AES session key using their RSA private key. Using the decrypted AES key, the ciphertext blocks are decrypted. Blockchain verification is performed simultaneously to confirm ciphertext integrity before plaintext recovery.

3.3 Algorithmic Workflow

The encryption and decryption processes of the proposed hybrid cryptosystem are detailed in the following algorithms.

```
Algorithm 1: Encryption Algorithm using AES+RSA+Blockchain
Inputs:
        •  Plaintext P
        •  Recipient RSA public key Kpub
        Outputs:
        •  BlockchainCipher (list of ciphertext blocks with hash links)
        •  Encrypted AES session key Kenc
        Steps:
          1.Generate a random AES session key $K_{AES}$
          2.Split the plaintext P into nfixed-size blocks $B_1,B_2,…,B_n$
          3.Initialize hash for first block H0=0 (genesis hash)
          4.For each block $B_i$ (i = 1 to n):
               4.1. Generate a random initialization vector (IV)
               4.2 Encrypt $B_i$ using AES-CBC with $K_{AES}$ and IV to get $C_i$
               4.3. Compute hash link: $Hi=Hash(Ci\|Hi-1)$
               4.4. Construct CipherBlock $CB_i=(Ci,IV,H_{i-1})$
               4.5. Append $CB_i$ to BlockchainCipher
            5.Encrypt the AES session key with RSA:
                 $K_{enc}=RSA\_Encrypt(K_{AES},K_{pub})$
        Output:
          •  BlockchainCipher = $[CB_1, CB_2, …, CB_n]$
          •  Encrypted AES key $K_{enc}$
     Algorithm 2: Decryption Algorithm using AES+RSA+Blockchain
        Inputs:
        •  BlockchainCipher = $[CB_1, CB_2, …, CB_n]$
        •  Encrypted AES session key $K_{enc}$
        •  Recipient RSA private key $K_{priv}$
        Outputs:
        •  Reconstructed plaintext PPP (Myanmar text)
        Steps:
          1.Decrypt the AES session key:$K_{AES}=RSA\_Decrypt(K_{enc},K_{priv})$
          2.Initialize hash for verification:H0=0
          3.Verify and decrypt each ciphertext block $CB_i$(i = 1 to n):
                3.1.Extract $(C_i,IV_i,H_{i-1})$ from CBi
                3.2. Verify blockchain integrity:
                        o  Compute expected hash:$H_i=Hash(C_i\|H_{i-1})$
                        o  If any computed hash does not match the stored link, **abort** (tampering detected)
                           3.3 Decrypt ciphertext block:$B_i=AES\_Decrypt(C_i,K_{AES},IV_i)$
                3.4 Append $B_i$ to plaintext reconstruction
            4. Concatenate all decrypted blocks to recover original plaintext P
            Output:
          •     Decrypted Myanmar plaintext P
```

4. Experimental Results and Performance Evaluation

The proposed AES+RSA+Blockchain hybrid cryptosystem for Myanmar text was implemented in Python 3.11 and tested on a workstation with Intel Core i7, 16 GB RAM, and Windows 10. Myanmar text samples of sizes 1 KB, 10 KB, 50 KB, and 100 KB were used, containing a variety of consonants, vowels, medials, and stacked characters to validate accurate language-aware encryption and decryption.
The system performance was evaluated using three key metrics: time efficiency, storage overhead, and security analysis.

4.1 Time Efficiency

Time efficiency evaluates how quickly the system can encrypt and decrypt Myanmar text of different sizes. This metric is critical for real-time secure communication applications such as e-government services and online banking. Table 2 presents the encryption and decryption times for various file sizes. Encryption time includes preprocessing, AES block encryption, RSA session key encryption, and blockchain construction. Decryption time includes RSA session key decryption, blockchain hash verification, and AES block decryption. Both encryption and decryption times increase linearly with file size, confirming the scalability of the system. Decryption is slightly faster than encryption because blockchain hash generation is only required during encryption.

Table 2- Time Efficiency of Proposed AES+RSA+Blockchain System

File Size (KB)	Encryption Time (ms)	Decryption Time (ms)
1	5	4
10	12	11
50	38	35
100	76	71

4.2 Storage Overhead

The blockchain structure introduces additional storage requirements due to the inclusion of initialization vectors (IVs) and hash values for each ciphertext block.Table 3 shows the average storage overhead for different file sizes, measured as the percentage increase compared to the original plaintext size. Each ciphertext block stores an IV (16 bytes) and a SHA-256 hash (32 bytes) of the previous block. The overhead decreases proportionally for larger files because fixed-size metadata becomes less significant as block count grows.The 7–8% overhead is acceptable for secure communications considering the added benefit of tamper detection.

Table 3- Storage Overhead of Blockchain-based Ciphertext

File Size (KB)	Ciphertext Size (KB)	Overhead (%)
1	1.08	8%
10	10.75	7.5%
50	53.50	7%
100	107.50	7.5%

4.3 Security Analysis

The security of the proposed hybrid cryptosystem was evaluated against confidentiality, integrity, and resistance to common attacks. Table 4 summarizes the security features and resistance of the system. Confidentiality is guaranteed by AES-256, which secures the plaintext against brute-force attacks. RSA-2048 ensures secure session key distribution, eliminating the traditional key-exchange vulnerability of symmetric systems.Blockchain integration provides tamper-evident ciphertext storage, enabling instant detection of unauthorized modifications or replay attempts.The combination of AES+RSA+Blockchain offers robust hybrid security for Myanmar-language text transmission.

Table 4- Security Analysis of Proposed Hybrid Cryptosystem

Security Feature	Mechanism Used	Evaluation Result
Confidentiality	AES-256 (symmetric encryption)	Strong encryption; resistant to brute-force attacks
Secure Key Distribution	RSA-2048 (asymmetric encryption)	Session key cannot be intercepted or forged
Integrity and Tamper Proof	Blockchain hash chaining	Any ciphertext modification is immediately detectable
Replay Attack Resistance	Immutable blockchain structure	Duplicate or reordered blocks are invalid
Brute-force Resistance	2^256 AES key space + RSA-2048	Infeasible for current computational power

5. Conclusion

This paper presented a hybrid cryptosystem that combines AES for fast symmetric encryption, RSA for secure key distribution, and blockchain forintegrity verification to secure Myanmar language text. The system addresses the unique challenges posed by Myanmar script, including its large character space and stacked diacritics, by implementing language-aware preprocessing before encryption. Experimental results demonstrate that the proposed AES+RSA+Blockchain framework achieves low encryption and decryption times, manageable storage overhead, and strong resistance to brute-force and tampering attacks. The integration of blockchain provides an additional layer of tamper detection, ensuring the reliability of encrypted communication in real-world applications such as e-government services, financial systems, and secure messaging platforms.

By bridging the gap between classical Myanmar cryptography and modern hybrid cryptosystems, this research contributes a practical, scalable, and security-enhanced solution for the secure transmission of Myanmar textual data.

References

Stallings, W. (2023). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson.

Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.

Htet, H., & Aye, M. (2020). Enhanced Beaufort cipher with stream cipher for Myanmar text encryption. Journal of Computer Applications, 12(4), 45–52.

Aung, T., & Hla, S. (2021). Vigenère-Affine hybrid cipher for Myanmar language cryptography. International Conference on Information Security and Language Processing, 88–94.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available: https://bitcoin.org/bitcoin.pdf

National Institute of Standards and Technology (NIST). (2001). Advanced Encryption Standard (AES) (FIPS PUB 197).

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.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. Proceedings of IEEE BigData Congress, 557–564.

Liu, Y., Li, Y., & Ma, J. (2020). Blockchain-based secure data storage for cloud and IoT. Journal of Information Security and Applications, 54, 102590.

Hossain, M. S., & Muhammad, G. (2020). Cloud-assisted industrial internet of things (IIoT)–enabled framework for health monitoring. IEEE Internet of Things Journal, 7(8), 8016–8023.