Secured Myanmar Text Using Symmetric Key Cryptography and BlockChain

Tin Thein Thwel
Cyber Security Research Lab,
Faculty of Information Sience
University of Computer Studies,
Yangon(UCSY)
Yangon, Myanmar
tintheinthwel@ucsy.edu.mm

May Theingi Kyaw
Cyber Security Research Lab,
Faculty of Information Sience
University of Computer Studies,
Yangon(UCSY)
Yangon, Myanmar
maytheingikyaw@ucsy.edu.mm

Myat Min Khant
Cyber Security Research Lab,
Faculty of Information Sience
University of Computer Studies,
Yangon(UCSY)
Yangon, Myanmar
myatminkhant1@ucsy.edu.mm

***Abstract*—Currently, working with Myanmar language encryption and decryption presents several challenges and considerations. These include accurately representing the wide range of Myanmar characters, ensuring consistent character encoding, managing encryption keys securely, selecting appropriate encryption algorithms, designing a user-friendly interface, rigorous testing and validation, performance optimization, adherence to security best practices, and providing clear documentation and support. Addressing these challenges requires careful planning, ongoing maintenance, and staying informed about advancements in encryption tools and libraries that may enhance support for the Myanmar language. This research work intends to fulfil such issues as preliminary step toward coping the above challenges. This work implemented the secure Myanmar language text using customized symmetric key cryptography and simple cipher blockchain technology.**

Keywords—Myanmar Language Cryptography, blockchain, symmetric key cryptography

I. INTRODUCTION

Secret key encryption, rooted in historical practices like the Caesar Shift Cipher during the Roman Empire, became vulnerable due to its limited 26-character alphabet, making it susceptible to brute force attacks. Early encryption methods, including the Spartans' Scytale and steganography, predated the Caesar cipher but were relatively simple and decipherable. The Pigpen Cipher, predating 1531, used symbols for substitution but was easily recognized due to its small symbol set. The Enigma code, initially formidable, was eventually cracked. Polyalphabetic ciphers like the Vigenère cipher and the Playfair Cipher introduced complexity, but the latter faced replacement due to keyword interception risks [1]. Thomas Jefferson's Jefferson Wheel Cipher, though inventive, was not widely adopted, and its reinvention as the M-94 cipher in the 20th century faced limitations due to its small wheel size [6]. The Data Encryption Standard (DES), published by NIST, set encryption standards but had a key length of 56 bits, making it vulnerable to brute force attacks [7]. Advanced Encryption Standard (AES), designed by Belgian cryptographers, is widely used but applies a consistent encryption approach for every block, potentially posing security risks [5].

II. RELATED WORK

The researchers, N. H. Htet and Z. M. Aye emphasizes the growing significance of information security in the digital era and the necessity for secure communication in languages like Myanmar. They introduced the Beaufort cipher as an initial encryption method and proposes an innovative approach by amalgamating it with the Stream cipher, a modern encryption technique, to enhance the security of Myanmar language communication. They proposed algorithm combines the Beaufort substitution cipher with the Stream cipher, resulting in distinct ciphertext segments that obfuscate the connection between ciphertext and plaintext, ultimately bolstering security. However, the exclusive use of Myanmar characters and the exclusion of Pali characters, they stated that the Beaufort cipher is relatively unsophisticated and vulnerable to attacks [3].

In response to these weaknesses, T. M. Aung and N. N. Hla, introduced the Vigenère-Affine cipher, a polyalphabetic encryption method that merge the Vigenère cipher with the Affine cipher to bolster security [4]. However, the Vigenère-Affine cipher combination increased complexity, which enhances security but can also complicate encryption and decryption processes if not implemented carefully. Balancing security and complexity is essential for effective use. Furthermore, the vigenère cipher, even in English alphabets, it has been found to be susceptible to Kasiski and Friedman attacks that rely on analyzing letter frequencies, rendering it less secure.

In this research work, we emphasize on Myanmar Language Cryptography to get stronger encryption and decryption algorithms in two Algorithms:

Algorithm-I: the simple cipher blockchain algorithm for Myanmar language cryptography.

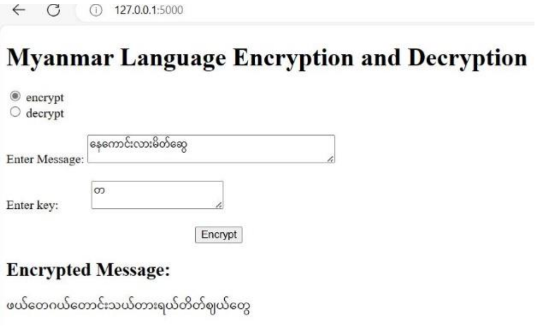
Algorithm-II: Cipher blockchain with key sequence to get stronger encryption and decryption algorithm for Myanmar language cryptography.

III. Proposed Algorithms

This work intends to propose and implement the Myanmar Language Encryption using the symmetric key cryptography and cipher blockchain. Myanmar language have unique characteristics significantly differentiate it from English and affect encryption practices. Myanmar Language encompasses 33 consonants, 12 vowels, and 4 medial, each represented by distinct symbols, in addition to unique diacritical marks. These elements create a vastly larger character set compared to the 26-letter English alphabet. Consequently, Myanmar Language encryption necessitates specialized techniques that accommodate this intricate character diversity, making it a fundamentally distinct encryption challenge. The Myanmar language's complexity underscores the need for language-specific considerations in encryption methods to ensure the secure transmission of information in this linguistic context. Therefore, this paper tried to propose and implement the custom symmetric encryption algorithm specifically designed for the Myanmar language using cipher blockchain [5]. The system is implemented with python with web application interface.

A. Encryption Algorithm –I using Cipher Blockchain:

```
Inputs: plaintext (P), key (K), blockSize (N)
1.  Split P into blocks of size N
2.  Initialize ciphertext (C) and blockchain (B) as empty
    lists
3.  For each block:
      3.1 Encrypt block using CBC_encrypt(block, K, IV)
      3.1.1 If first block, use randomIV() as IV
      3.2 Create CipherBlock(encryptedBlock, K, IV)
      3.3 Append CipherBlock to B
      3.4 Set IV = encrypted block
4.  C = concatenateBlocks(B)
5.  Return C
```



127.0.0.1:5000

Myanmar Language Encryption and Decryption

● encrypt
○ decrypt

Enter Message: နေကောင်းလားမိတ်ဆွေ

Enter key: တ

Encrypt

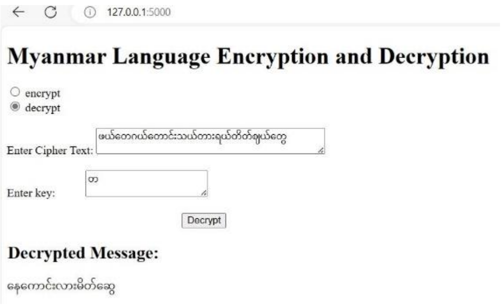
Encrypted Message:

ဖယ်တေဂယ်တောင်းသယ်တားရယ်တိတ်ဈယ်တွေ

Fig. 1. Encryption Result.

B. Decryption Algorithm-I using Cipher Blockchain:

```
Inputs: ciphertext (C), key (K), blockSize (N)
1.  B = splitIntoBlocks(C, blockSize)
2.  P = ""
3.  For each CipherBlock CB in B:
      3.1 Decrypt block using CBC_decrypt
          (CB.encryptedblock, CB.K,  CB.IV)
      3.2 Append decrypted block to P
      3.3 Set IV = CB.encryptedBlock
4.  Return P
```



127.0.0.1:5000

Myanmar Language Encryption and Decryption

○ encrypt
● decrypt

Enter Cipher Text: ဖယ်တေဂယ်တောင်းသယ်တားရယ်တိတ်ဈယ်တွေ

Enter key: တ

Decrypt

Decrypted Message:

နေကောင်းလားမိတ်ဆွေ

Fig. 2. Decryption Result.

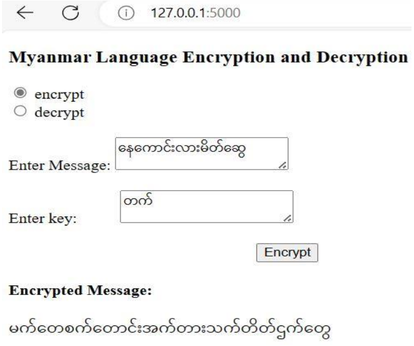
This is the preliminary step we tried and it is hard to do the frequent analysis. However, if the skilled cryptanalyst can break it with brute force attack if he/she know the Myanmar consonants, vowels and medial. The time complexity for the brute force attack will as shown bellows:

$$\mathrm{O}(n) \ = CxVxM \tag{1}$$

Where, C is number of consonants, V is number of vowels and M is the number of medial. So we tried to improve the Algorithm-I with initial vector, key consonant with vowel and medial instead of using only one consonant as a key.

C. Encryption Algorithm-II using Cipher Blockchain:

```
Input: plaintext (P), key (K), blockSize (N)
1.  Initialize ciphertext (C) and blockchain (B) as empty
2.  While P is not empty:
      2.1 Take next block of P of size N
      2.2 Encrypt block using CBC encryption(block, K, IV)
      2.2.1 If first block, use randomIV() as IV
      2.3 Create CipherBlock(encryptedBlock, K, IV)
      2.4 Append CipherBlock to blockchain B
      2.5 Set K = hash(K)
      2.6 Remove block from P
3.  Return concatenateBlockchain(B) as ciphertext
```



127.0.0.1:5000

Myanmar Language Encryption and Decryption

● encrypt
○ decrypt

Enter Message: နေကောင်းလားမိတ်ဆွေ

Enter key: တက်

Encrypt

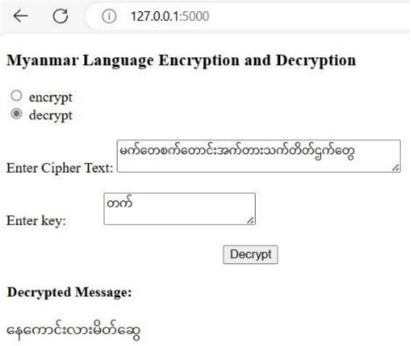
Encrypted Message:

မက်တေစက်တောင်းအက်တားသက်တိတ်ဌက်တွေ

Fig. 3. Encryption Result

D. Decryption Algorithm-II using Cipher Blockchain:

```
Input: ciphertext (C), key (K), blockSize (N)
1.  B = splitIntoBlocks(C, blockSize)
2.  P = ""
3.  For each block in B:
        3.1 CB = getCipherBlock(block)
        3.2 block = CBCdecryption(CB.encryptedBlock,
        CB.K, CB.IV)
        3.3 P = P + block
        3.4 Set IV = CB.encryptedBlock
        3.5 Set K = hash(K)
4.  Return P
```



Myanmar Language Encryption and Decryption

○ encrypt
● decrypt

Enter Cipher Text: မက်တေစက်တောင်းအက်တားသက်တိတ်ဌက်တွေ

Enter key: တက်

Decrypted Message:

နေကောင်းလားမိတ်ဆွေ

Fig. 4. Decryption Result

Where, IV is initial vector, CBCencryption(block, K, IV) encrypts a single plaintext block using CBC mode, CBCdecryption(encryptedBlock, K, IV) decrypts a single ciphertext block using CBC mode, concatenateBlockchain(B) joins all cipher blocks in the blockchain into a single ciphertext, splitIntoBlocks(C,blockSize) splits ciphertext into blocks, getCipherBlock(block) retrieves the cipher block object from an encrypted block, hash(K) derives a new key for the next block via crypto-hashing, randomIV() generates a secure random initialization vector.

According to the implementation, Encryption/Decryption Algorithm-II takes a more robust approach to key and IV handling that strengthens the cipher against related-key and chosen-IV attacks. The explicit key hashing also adds confusion between blocks. So in terms of which algorithm presents a stronger security model based on the details given, Encryption/Decryption Algorithm-II has an advantage due to its approach to key derivation and IV generation from the ciphertext.

IV. Performance Evaluation

The previous research works [3][4] concerned with Myanmar Language Encryptions are based on the Unicode equivalent value with proposed Myanmar-Vigenère Table. However, in this research work, the encryption is done upon the Myanmar text and characters and not on the Unicode equivalent value. In addition, the performance criteria for the encryption algorithm are security, speed and efficiency. Hence, in this research work, the performance is evaluated in terms of security, that is, discussed in Section III, and speed which is discussed below.

A. *Time Comparison for the algorithms*

The time comparison results for Encryption Algorithm-I, Decryption Algorithm-I, Encryption Algorithm-II, and Decryption Algorithm-II is described in Table I.

TABLE I. Time Comparison for the algorithms

Time	**Algorithm-I**	**Algorithm-II**
	IV and Single Consonant Key	***IV and Consonant with Vowel and Medial Key***
Encryption	0.00354766845703125 s	0.003908872604370117 s
Decryption	0.24205422401428223 s	0.003020048141479492 s

Plain Text for Algorithm-I: နေကောင်းလားမိတ်ဆွေ

Key: တ

Plain Text for Algorithm-II: နေကောင်းလားမိတ်ဆွေ

Key: တက်

According to the experiment results, even the Algorithm-II is more robust with initial vector and consonant with vowel and medial key combination, the execution time is faster than Algorithm-I.

V. Conclusion

In conclusion, the research dig into block cipher-based encryption and decryption algorithms. These algorithms ensured the secure encryption of plaintext blocks through an iterative process using CBC mode, incorporating a random initialization vector and a robust key. The encrypted blocks were stored as cipher objects, encompassing both ciphertext and keys. On the decryption side, the process was reversed, involving the decryption of blocks using CBC mode and the reassembly of plaintext. Throughout this endeavor, auxiliary functions managed essential tasks like AES encryption/decryption of blocks, key derivation, vector generation, and data transformations. By presenting these algorithms conceptually, the study highlighted the significance of factors such as unpredictable inputs and the interlinking of keys between blocks, which collectively bolstered security. These insights have broader implications for the design of contemporary encryption systems, including potential applications in the realm of Myanmar language encryption.

References

[1] S. Chandra, S. Bhattacharyya, S. PairaSmita, and Sk. S. Alam, “A Study and Analysis on Symmetric Cryptography,” in International Conference on Science, Engineering and Management Research (ICSEMR 2014), India, pp. 1–8, 2014.

[2] P. G. Patil, V. K. Verma, “A Recent Survey on Different Symmetric Key” in International Journal of Computing and Technology, Volume 3, Issue 2, February 2016.

[3] N. H. Htet and Z. M. Aye, “Innovation Security of Beaufort Cipher by Stream Cipher Using Myanmar-Vigenere Table and Unicode Table,” in Proceedings of the 10th International Workshop on Computer Science and Engineering (WCSE 2020), Shanghai, China, p. 52-26, 2020.

[4] T. M. Aung and N. N. Hla, “A Complex Polyalphabetic Cipher Technique Myanmar Polyalphabetic Cipher,” 2019 International Conference on Computer Communication and Informatics (ICCCI), India, pp. 1-9, 2019

[5] O. Lage et al., “Computer Security Threats: Blockchain Applications in Cybersecurity”,Open access peer-review chapter, 2019.

[6] https://www.monticello.org/site/research-and-collections/wheel-cipher

[7] https://searchsecurity.techtarget.com/definition/Data-Encryption-standard