Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
6 (1) 2026, Page: 18121-18132

TEXT MESSAGE ENCRYPTION AND DECRYPTION MODEL USING PERMUTATION MATRIX CONSTRUCTION OVER MAX-PLUS ALGEBRA

Igin Antadi[1], Nurwan[2], Armayani Arsal[3], Djihad Wungguli[4], Nisky Imansyah Yahya[5]

[1,2,3,4,5] **Faculty of Mathematics and Natural Sciences Mathematics Department, Negeri Gorontalo University**

Corresponding Author: **Igin Antadi, e-mail: igin.antadi07@gmail.com**

Published: Maret , 2026

ABSTRAK

Studi ini membahas kelemahan sistem kriptografi berbasis matriks sirkulan tropis, yang masih menunjukkan pola berulang dan ruang kunci terbatas, sehingga rentan terhadap serangan berbasis pola. Untuk mengatasi masalah ini, dikembangkan model enkripsi dan dekripsi pesan teks menggunakan konstruksi matriks permutasi dalam aljabar Max-Plus. Model ini dirancang untuk secara konsisten membangun kunci rahasia bersama melalui proses pertukaran kunci dan untuk memastikan keamanan pesan teks. Pendekatan studi ini mencakup tinjauan pustaka, desain algoritma enkripsi dan dekripsi dalam semiring Max-Plus, dan implementasi melalui simulasi numerik. Proses simulasi dilakukan untuk mengevaluasi ketahanan model terhadap serangan dan efisiensi komputasinya. Temuan menunjukkan bahwa penggunaan matriks permutasi secara efektif meningkatkan keamanan sistem dengan memperluas ruang pencarian kunci dan menghilangkan pola berulang yang umum ditemukan dalam model sirkulan. Model yang diusulkan mampu melakukan proses enkripsi dan dekripsi yang stabil dan akurat di berbagai ukuran matriks. Namun, peningkatan ukuran matriks menyebabkan waktu komputasi yang lebih tinggi, menunjukkan perlunya keseimbangan antara keamanan dan efisiensi. Secara keseluruhan, studi ini menunjukkan bahwa konstruksi matriks permutasi dalam aljabar Max-Plus memiliki potensi signifikan untuk dikembangkan sebagai dasar sistem kriptografi modern yang aman, efisien, dan adaptif terhadap ancaman komputasi di masa depan.

Kata Kunci: Aljabar Max-Plus, Matriks Permutasi, Enkripsi Pesan, Dekripsi Pesan, Kriptografi Tropis

ABSTRACT

This study addresses the weaknesses of cryptographic systems based on tropical circulant matrices, which still exhibit repetitive patterns and limited key spaces, making them vulnerable to pattern-based attacks. To overcome these issues, a text message encryption and decryption model is developed using permutation matrix constructions in Max-Plus algebra. This model is designed to consistently establish a shared secret key through a key exchange process and to ensure the security of text messages. The study's approach includes a literature review, the design of encryption and decryption algorithms within the Max-Plus semiring, and implementation through numerical simulations. Simulation processes are conducted to evaluate the model's resistance to attacks and its computational efficiency. The findings demonstrate that the use of permutation matrices effectively enhances system security by expanding the key search space and eliminating repetitive patterns commonly found in circulant models. The proposed model is capable of performing stable and accurate encryption and decryption processes across various matrix sizes. However, increasing matrix size leads to higher computational time, indicating the need for a balance between security and efficiency. Overall, this study demonstrates that permutation matrix constructions in Max-Plus algebra have significant potential to be developed as the foundation of modern cryptographic systems that are secure, efficient, and adaptive to future computational threats.

Keywords: Max-plus algebra, permutation matrix, message encryption, message decryption, tropical cryptography

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

INTRODUCTION

In the rapidly developing digital era, data security has become a crucial aspect in various sectors such as communication, banking, and government. The advancement of information and communication technology has transformed the way humans interact, work, and conduct financial transactions. Along with the increasing volume of data exchanged online, threats to information security have become increasingly complex. Information transmitted through networks can become targets of cyberattacks, either by individuals or groups with specific interests. Common types of attacks include personal data theft, identity falsification, and system hacking, which can result in financial losses and the leakage of confidential information. These threats continue to intensify in line with technological advancements that enable cybercriminals to employ increasingly sophisticated methods to exploit security vulnerabilities in information systems (Huang et al., 2022).

Cryptography is a branch of science that studies techniques for securing information through mathematical transformations, so that only parties with specific authorization can understand the content of the message. In its application, cryptography employs encryption (encoding) and decryption (message recovery) processes by utilizing specific keys (Article, 2023). Along with the advancement of technology, classical cryptographic schemes such as *RSA* and *ECC* are increasingly considered insufficiently secure against potential quantum computing–based attacks. Therefore, new approaches that are more adaptive to future threats are required (Huang et al., 2022). One alternative that has begun to be explored is the use of non-conventional mathematical structures, such as Max-Plus algebra, which offer a new approach to constructing modern cryptographic systems.

Max-Plus algebra is a tropical semiring in which the addition operation is replaced by the maximum operation, and the multiplication operation is replaced by ordinary addition. This structure creates a unique mathematical system that is potentially powerful in obscuring encryption patterns. In addition to being computationally efficient, Max-Plus algebra is also difficult to analyze using conventional cryptanalytic techniques (Durcheva, 2022). In this context, tropical matrix structures such as circulant matrices have been utilized in various key exchange protocols and encryption systems, including the *Huang and Deng protocol*, two versions of the *Amutha and Perumal protocol*, as well as the *TrES* protocol developed by *Durcheva*. These four protocols demonstrate that the combination of tropical matrix structures and Max-Plus algebraic operations can form an efficient cryptographic system.

However, research (Of et al., 2023), indicates that although circulant matrix structures support computational efficiency, such systems possess fundamental weaknesses in the form of recurring patterns and a limited key space due to their deterministic nature. The reliance on a single initial row as the basis for generating all matrix elements causes the transformation patterns to be easily predictable, thereby opening opportunities for pattern-based attacks and structural reconstruction. To address these weaknesses, a new approach is required that is capable of producing matrix transformations that are more random and free from discernible patterns.

One potential solution is the use of permutation matrices in the Max-Plus semiring. Unlike circulant matrices, permutation matrices do not exhibit cyclic patterns and rearrange the elements of a vector in a random manner. This increases the level of text message confidentiality while simultaneously enhancing the system's resistance to structural exploitation. Therefore, this study aims to develop an encryption and decryption model based on permutation matrices in the Max-Plus semiring as a modification of previous models that employ tropical circulant matrices. This modification is expected to improve data security without compromising computational efficiency (Huang et al., 2022).

In addition, this study also addresses the integration of permutation matrix–based encryption models with secure communication protocols based on tropical algebra. The model is evaluated through numerical simulations and experimental analysis to assess the effectiveness of the proposed method in terms of resistance to cryptanalysis, computational efficiency, and reliability in preserving message confidentiality (Muanalifah, n.d.). Thus, this study is expected to contribute to the development of modern cryptographic systems based on tropical algebra that are more robust and resilient to future computational threats.

METHOD

The research methodology begins with a literature study to examine the concepts of Max-Plus algebra–based cryptography, permutation matrices, and secure communication protocols, as well as to analyze the weaknesses of tropical circulant matrix–based models. Subsequently, an encryption and decryption model is designed using permutation matrices in the Max-Plus semiring through the development of appropriate algorithms. The developed model is then tested through numerical simulations using manual methods to evaluate its effectiveness. Further analysis is conducted to assess the model's resistance to cryptanalytic attacks and to evaluate its efficiency in comparison with previous encryption methods, in order to ensure an optimal level of security and performance.

FINDING AND DISCUSSION

Implementation of the huang protocol based on circulant matrices in max-plus algebra

he implementation of the Huang protocol in this study utilizes circulant matrices as cryptographic keys within the Max-Plus algebra framework, as introduced by (Huang et al., 2022). The implementation process generally consists of three main stages, namely key exchange, encryption, and decryption. During the key exchange stage, both parties generate a shared secret key through Max-Plus matrix multiplication operations on a public matrix without revealing their private keys. Subsequently, the shared key is used in the encryption and decryption processes to secure numerical messages, where the success of the protocol is demonstrated when the decryption result is identical to the original message. To provide a clearer illustration, the algorithm used in each stage is presented below.

Algorithm 1: Key Exchange, Encryption, and Decryption

Input: Public Matrix $Y \epsilon R_{max}^{3\times3}$, secret circulant matrix $(P_1, Q_1), (P_2, Q_2)$, text message M

Output: Ciphertext S and decrypted plaintext M

1. **Key Exchange:**
   - **a)** Alice and Bob agree on Y
   - **b)** Alice computes $K_A = P_1 \otimes Y \otimes Q_1$; Bob computes $K_B = P_2 \otimes Y \otimes Q_2$
   - **c)** Alice and Bob exchange K_A, K_B
   - **d)** Shared key: $K = P_1 \otimes K_B \otimes Q_1 = P_2 \otimes Y \otimes Q_2$
2. **Encryption**
   - **a)** The message M is divided into 3×3 blocks and converted into ASCII
   - **b)** Bob computes $R = P_2 \otimes Y \otimes Q_2$ and $T = P_2 \otimes K_A \otimes Q_2$
   - **c)** Chipertext: $S = M + T$
   - **d)** Bob sends the pair (S, R)
3. **Dekripsi:**
   - **a)** Alice computes $T = P_1 \otimes R \otimes Q_1$
   - **b)** Original message: $M = S - T$
   - **c)** Convert the ASCII values of M back into text characters

Example of the huang protocol based on circulant matrices in max-plus algebra

1. **Key Exchange**
   - **a)** Initialization: Alice and Bob agree on a public matrix $Y \epsilon R_{max}^{3\times3}$ namely:

$$Y = \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix}$$

   - **b)** Key generation: Alice and Bob
     - Alice selects the circulant matrices P_1 and Q_1

$$P_1 = \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix}, Q_1 = \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix}$$

Then computes:

$$K_A = P_1 \otimes Y \otimes Q_1$$

$$K_A = \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix} \otimes \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix}$$

$$K_A = \begin{bmatrix} 243 & 255 & 246 \\ 208 & 232 & 244 \\ 223 & 197 & 211 \end{bmatrix}$$

- Bob selects the circulant matrices P_2 and Q_2

$$P_2 = \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix}, Q_2 = \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix}$$

Then computes:

$$K_B = P_2 \otimes Y \otimes Q_2$$

$$K_B = \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix} \otimes \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix}$$

$$K_B = \begin{bmatrix} 257 & 248 & 222 \\ 218 & 246 & 192 \\ 211 & 207 & 225 \end{bmatrix}$$

c) Shared key

- Alice computes:

$$K_{AB} = P_1 \otimes K_B \otimes Q_1$$

$$K_{AB} = \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix} \otimes \begin{bmatrix} 257 & 248 & 222 \\ 218 & 246 & 192 \\ 211 & 207 & 225 \end{bmatrix} \otimes \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix}$$

$$K_{AB} = \begin{bmatrix} 378 & 380 & 392 \\ 424 & 415 & 412 \\ 401 & 413 & 377 \end{bmatrix}$$

- Bob computes:

$$K_{BA} = P_2 \otimes K_A \otimes Q_2$$

$$K_{BA} = \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix} \otimes \begin{bmatrix} 243 & 255 & 246 \\ 208 & 232 & 244 \\ 223 & 197 & 211 \end{bmatrix} \otimes \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix}$$

$$K_{BA} = \begin{bmatrix} 378 & 380 & 392 \\ 424 & 415 & 412 \\ 401 & 413 & 377 \end{bmatrix}$$

Conclusion:

$$K = K_{AB} = K_{BA} = \begin{bmatrix} 378 & 380 & 392 \\ 424 & 415 & 412 \\ 401 & 413 & 377 \end{bmatrix}$$

2. Encryption

a) Message preparation

Bob's message: "AKU SUKA MATEMATIKA" is divided into three 3 × 3 blocks (ASCII conversion):

$$M_1 = \begin{bmatrix} 65 & 75 & 85 \\ 32 & 83 & 85 \\ 75 & 65 & 32 \end{bmatrix}, M_2 = \begin{bmatrix} 77 & 65 & 84 \\ 69 & 77 & 65 \\ 84 & 73 & 75 \end{bmatrix}, M_3 = \begin{bmatrix} 65 & 48 & 48 \\ 48 & 48 & 48 \\ 48 & 48 & 48 \end{bmatrix}$$

b) Selection of circulant matrices

- Block 1

$$P_{2,1} = \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix}, Q_{2,1} = \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix}$$

- Block 2

$$P_{2,2} = \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix}, Q_{2,2} = \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix}$$

- Block 3

$$P_{2,3} = \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix}, Q_{2,3} = \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix}$$

c) Compute the ciphertext using:

- Block 1
  1) Compute the temporary matrix:

$$R_1 = P_{2,1} \otimes Y \otimes Q_{2,1}$$

$$R_1 = \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix} \otimes \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix}$$

$$R_1 = \begin{bmatrix} 232 & 233 & 193 \\ 188 & 221 & 212 \\ 244 & 235 & 205 \end{bmatrix}$$

  2) Compute the session key component

$$T_1 = P_{2,1} \otimes K_A \otimes Q_{2,1}$$

$$T_1 = \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix} \otimes \begin{bmatrix} 243 & 255 & 246 \\ 208 & 232 & 244 \\ 223 & 197 & 211 \end{bmatrix} \otimes \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix}$$

$$T_1 = \begin{bmatrix} 411 & 402 & 399 \\ 399 & 400 & 387 \\ 376 & 388 & 379 \end{bmatrix}$$

  3) Chipertext:

$$S_1 = M + T \text{ } \textit{(element-wise addition)}$$

$$S_1 = \begin{bmatrix} 65 + 411 & 75 + 402 & 85 + 399 \\ 32 + 399 & 83 + 400 & 85 + 387 \\ 75 + 376 & 65 + 388 & 32 + 379 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 476 & 477 & 484 \\ 431 & 483 & 472 \\ 451 & 453 & 411 \end{bmatrix}$$

- Block 2
  1) Compute the temporary matrix

$$R_2 = P_{2,2} \otimes Y \otimes Q_{2,2}$$

$$R_2 = \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix} \otimes \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix}$$

$$R_2 = \begin{bmatrix} 257 & 248 & 222 \\ 218 & 246 & 192 \\ 211 & 207 & 225 \end{bmatrix}$$

  2) Compute the session key component

$$T_2 = P_{2,2} \otimes K_A \otimes Q_{2,2}$$

$$T_2 = \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix} \otimes \begin{bmatrix} 243 & 255 & 246 \\ 208 & 232 & 244 \\ 223 & 197 & 211 \end{bmatrix} \otimes \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix}$$

$$T_2 = \begin{bmatrix} 378 & 380 & 392 \\ 424 & 415 & 412 \\ 401 & 413 & 377 \end{bmatrix}$$

  3) Chipertext

$$S_2 = M + T \text{ } \textit{(element-wise addition)}$$

$$S_2 = \begin{bmatrix} 77 + 378 & 65 + 380 & 84 + 392 \\ 69 + 424 & 77 + 415 & 65 + 412 \\ 84 + 401 & 73 + 413 & 75 + 377 \end{bmatrix}$$

$$S_2 = \begin{bmatrix} 455 & 445 & 476 \\ 493 & 492 & 477 \\ 485 & 486 & 452 \end{bmatrix}$$

- Block 3
  1) Compute the temporary matrix

$$R_3 = P_{2,3} \otimes Y \otimes Q_{2,3}$$

$$R_3 = \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix} \otimes \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix}$$

$$R_3 = \begin{bmatrix} 232 & 244 & 235 \\ 193 & 221 & 233 \\ 212 & 198 & 200 \end{bmatrix}$$

2) Compute the session key component

$$T_3 = P_{2,3} \otimes K_A \otimes Q_{2,3}$$

$$T_3 = \begin{bmatrix} 33 & 40 & 79 \\ 79 & 33 & 40 \\ 40 & 79 & 33 \end{bmatrix} \otimes \begin{bmatrix} 243 & 255 & 246 \\ 208 & 232 & 244 \\ 223 & 197 & 211 \end{bmatrix} \otimes \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix}$$

$$T_3 = \begin{bmatrix} 379 & 365 & 367 \\ 399 & 411 & 402 \\ 376 & 388 & 400 \end{bmatrix}$$

3) Chipertext

$S_3 = M + T$ *(element-wise addition)*

$$S_3 = \begin{bmatrix} 65 + 379 & 48 + 365 & 48 + 367 \\ 48 + 399 & 48 + 411 & 48 + 402 \\ 48 + 376 & 48 + 388 & 48 + 400 \end{bmatrix}$$

$$S_3 = \begin{bmatrix} 444 & 413 & 415 \\ 447 & 459 & 450 \\ 424 & 436 & 448 \end{bmatrix}$$

d) Transmission:

Send the pair *(S, R)* to Alice.

3. Decryption

a) Session key reconstruction

Alice Compute:

- Block 1

$$T_1 = P_1 \otimes R_1 \otimes Q_1$$

$$T_1 = \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix} \otimes \begin{bmatrix} 232 & 233 & 193 \\ 188 & 221 & 212 \\ 244 & 235 & 205 \end{bmatrix} \otimes \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix}$$

$$T_1 = \begin{bmatrix} 411 & 402 & 399 \\ 399 & 400 & 387 \\ 376 & 388 & 379 \end{bmatrix}$$

- Block 2

$$T_2 = P_1 \otimes R_2 \otimes Q_1$$

$$T_2 = \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix} \otimes \begin{bmatrix} 257 & 248 & 222 \\ 218 & 246 & 192 \\ 211 & 207 & 225 \end{bmatrix} \otimes \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix}$$

$$T_2 = \begin{bmatrix} 378 & 380 & 392 \\ 424 & 415 & 412 \\ 401 & 413 & 377 \end{bmatrix}$$

- Block 3

$$T_3 = P_1 \otimes R_3 \otimes Q_1$$

$$T_3 = \begin{bmatrix} 12 & 55 & 90 \\ 90 & 12 & 55 \\ 55 & 90 & 12 \end{bmatrix} \otimes \begin{bmatrix} 232 & 244 & 235 \\ 193 & 221 & 233 \\ 212 & 198 & 200 \end{bmatrix} \otimes \begin{bmatrix} 77 & 21 & 65 \\ 65 & 77 & 21 \\ 21 & 65 & 77 \end{bmatrix}$$

$$T_3 = \begin{bmatrix} 379 & 365 & 367 \\ 399 & 411 & 402 \\ 376 & 388 & 400 \end{bmatrix}$$

b) Plaintext recovery

Compute the original message block:

- Block 1

$$M_1 = S_1 - T_1$$

$$M_1 = \begin{bmatrix} 476 - 411 & 477 - 402 & 484 - 399 \\ 431 - 399 & 483 - 400 & 472 - 387 \\ 451 - 376 & 453 - 388 & 411 - 379 \end{bmatrix}$$

$$M_1 = \begin{bmatrix} 65 & 75 & 85 \\ 32 & 83 & 85 \\ 75 & 65 & 32 \end{bmatrix}$$

- Block 2

$M_2 = S_2 - T_2$

$$M_2 = \begin{bmatrix} 455-378 & 445-380 & 476-392 \\ 493-424 & 492-415 & 477-412 \\ 485-401 & 486-413 & 452-377 \end{bmatrix}$$

$$M_2 = \begin{bmatrix} 77 & 65 & 84 \\ 69 & 77 & 65 \\ 84 & 73 & 75 \end{bmatrix}$$

- Block 3

$M_3 = S_3 - T_3$

$$M_3 = \begin{bmatrix} 444-379 & 414-365 & 415-367 \\ 447-399 & 459-411 & 450-402 \\ 424-376 & 436-388 & 448-400 \end{bmatrix}$$

$$M_3 = \begin{bmatrix} 65 & 48 & 48 \\ 48 & 48 & 48 \\ 48 & 48 & 48 \end{bmatrix}$$

c) Text Conversion

Convert the ASCII values of M back into characters:

$$M_1 = \begin{bmatrix} A & K & U \\ (space) & S & U \\ K & A & (space) \end{bmatrix}, M_2 = \begin{bmatrix} M & A & T \\ E & M & A \\ T & I & K \end{bmatrix}, M_3 = \begin{bmatrix} A & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Implementation of the huang protocol based on permutation matrices in max-plus algebra

The implementation of the Huang protocol in this study is not only conducted using circulant matrices but is also compared with the use of permutation matrices in Max-Plus algebra operations. In general, the implementation stages in both models are divided into three main processes: key exchange, encryption, and decryption. The difference lies in the form of the key matrices used. In circulant matrices, the matrix elements are arranged cyclically, resulting in more varied patterns, whereas in permutation matrices, the elements consist only of 0 dan $-\infty$, making the structure simpler while still satisfying the fundamental properties of Max-Plus algebra, such as closure under Max-Plus multiplication $\otimes$, the existence of an identity matrix, and the possibility of forming an inverse through transposition, which is necessary for the decryption process. The algorithm used in each stage is presented below.

Algorithm 2: Key Exchange, Encryption, and Decryption

Input: Public Matrix $Y \epsilon R_{max}^{3\times3}$, secret permutation matrix $(P_1, Q_1), (P_2, Q_2)$, text message M

Output: Ciphertext S and decrypted plaintext M

1. **Key Exchange:**
   - **a)** Alice and Bob agree on Y
   - **b)** Alice computes $K_A = P_1 \otimes Y \otimes Q_1$; Bob computes $K_B = P_2 \otimes Y \otimes Q_2$
   - **c)** Alice and Bob exchange K_A, K_B
   - **d)** Shared key: $K = P_1 \otimes K_B \otimes Q_1 = P_2 \otimes Y \otimes Q_2$
2. **Encryption**
   - **a)** The message M is divided into 3×3 blocks and converted into ASCII
   - **b)** Bob computes $R = P_2 \otimes Y \otimes Q_2$ and $T = P_2 \otimes K_A \otimes Q_2$
   - **c)** Chipertext: $S = M + T$
   - **d)** Bob sends the pair (S,R)
3. **Dekripsi:**
   - **a)** Alice computes $T = P_1 \otimes R \otimes Q_1$
   - **b)** Original message: $M = S - T$
   - **c)** Convert the ASCII values of M back into text characters

Example of the huang protocol based on permutation matrices in max-plus algebra

1. **Key Exchange**

a) Initialization: Alice and Bob agree on a public matrix $Y \epsilon R_{max}^{3\times3}$ namely:

$$Y = \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix}$$

b) Key generation: Alice and Bob

- Alice selects the circulant matrices P_1 and Q_1

$$P_1 = \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix}, Q_1 = \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix}$$

Then computes:

$$K_A = P_1 \otimes Y \otimes Q_1$$

$$K_A = \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix} \otimes \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix}$$

$$K_A = \begin{bmatrix} 21 & 19 & 56 \\ 88 & 79 & 20 \\ 24 & 77 & 23 \end{bmatrix}$$

- Bob selects the circulant matrices P_2 and Q_2

$$P_2 = \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix}, Q_2 = \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix}$$

Then computes:

$$K_B = P_2 \otimes Y \otimes Q_2$$

$$K_B = \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix} \otimes \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix}$$

$$K_B = \begin{bmatrix} 77 & 23 & 24 \\ 19 & 56 & 21 \\ 79 & 20 & 88 \end{bmatrix}$$

c) Shared key

- Alice computes:

$$K_{AB} = P_1 \otimes K_B \otimes Q_1$$

$$K_{AB} = \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix} \otimes \begin{bmatrix} 77 & 23 & 24 \\ 19 & 56 & 21 \\ 79 & 20 & 88 \end{bmatrix} \otimes \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix}$$

$$K_{AB} = \begin{bmatrix} 56 & 21 & 19 \\ 20 & 88 & 79 \\ 23 & 24 & 77 \end{bmatrix}$$

- Bob computes:

$$K_{BA} = P_2 \otimes K_A \otimes Q_2$$

$$K_{BA} = \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix} \otimes \begin{bmatrix} 21 & 19 & 56 \\ 88 & 79 & 20 \\ 24 & 77 & 23 \end{bmatrix} \otimes \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix}$$

$$K_{BA} = \begin{bmatrix} 56 & 21 & 19 \\ 20 & 88 & 79 \\ 23 & 24 & 77 \end{bmatrix}$$

Conclusion:

$$K = K_{AB} = K_{BA} = \begin{bmatrix} 56 & 21 & 19 \\ 20 & 88 & 79 \\ 23 & 24 & 77 \end{bmatrix}$$

2. **Encryption**

a) Message preparation

Bob's message: "AKU SUKA MATEMATIKA" is divided into three 3 × 3 blocks (ASCII conversion):

$$M_1 = \begin{bmatrix} 65 & 75 & 85 \\ 32 & 83 & 85 \\ 75 & 65 & 32 \end{bmatrix}, M_2 = \begin{bmatrix} 77 & 65 & 84 \\ 69 & 77 & 65 \\ 84 & 73 & 75 \end{bmatrix}, M_3 = \begin{bmatrix} 65 & 48 & 48 \\ 48 & 48 & 48 \\ 48 & 48 & 48 \end{bmatrix}$$

b) Selection of circulant matrices

- Block 1

$$P_{2,1} = \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix}, Q_{2,1} = \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix}$$

- Block 2

$$P_{2,2} = \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix}, Q_{2,2} = \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix}$$

- Block 3

$$P_{2,3} = \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix}, Q_{2,3} = \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix}$$

c) Compute the ciphertext using:

- Block 1

1) Compute the temporary matrix:

$$R_1 = P_{2,1} \otimes Y \otimes Q_{2,1}$$

$$R_1 = \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix} \otimes \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix}$$

$$R_1 = \begin{bmatrix} 20 & 88 & 79 \\ 23 & 24 & 77 \\ 56 & 21 & 19 \end{bmatrix}$$

2) Compute the session key component

$$T_1 = P_{2,1} \otimes K_A \otimes Q_{2,1}$$

$$T_1 = \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix} \otimes \begin{bmatrix} 21 & 19 & 56 \\ 88 & 79 & 20 \\ 24 & 77 & 23 \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix}$$

$$T_1 = \begin{bmatrix} 24 & 77 & 23 \\ 21 & 19 & 56 \\ 88 & 79 & 20 \end{bmatrix}$$

3) Chipertext:

$$S_1 = M + T \text{ (element-wise addition)}$$

$$S_1 = \begin{bmatrix} 65+24 & 75+77 & 85+23 \\ 32+21 & 83+19 & 85+56 \\ 75+88 & 65+79 & 32+20 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 89 & 152 & 108 \\ 53 & 102 & 141 \\ 163 & 144 & 52 \end{bmatrix}$$

- Block 2

1) Compute the temporary matrix

$$R_2 = P_{2,2} \otimes Y \otimes Q_{2,2}$$

$$R_2 = \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix} \otimes \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix}$$

$$R_2 = \begin{bmatrix} 24 & 77 & 23 \\ 21 & 19 & 56 \\ 88 & 79 & 20 \end{bmatrix}$$

2) Compute the session key component

$$T_2 = P_{2,2} \otimes K_A \otimes Q_{2,2}$$

$$T_2 = \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix} \otimes \begin{bmatrix} 21 & 19 & 56 \\ 88 & 79 & 20 \\ 24 & 77 & 23 \end{bmatrix} \otimes \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix}$$

$$T_2 = \begin{bmatrix} 19 & 56 & 21 \\ 79 & 20 & 88 \\ 77 & 23 & 24 \end{bmatrix}$$

3) Chipertext

$$S_2 = M + T \text{ (element-wise addition)}$$

$$S_2 = \begin{bmatrix} 77+19 & 65+56 & 84+21 \\ 69+79 & 77+20 & 65+88 \\ 84+77 & 73+23 & 75+24 \end{bmatrix}$$

$$S_2 = \begin{bmatrix} 96 & 121 & 105 \\ 148 & 97 & 153 \\ 161 & 96 & 99 \end{bmatrix}$$

- Block 3
  1) Compute the temporary matrix
  $R_3 = P_{2,3} \otimes Y \otimes Q_{2,3}$
  $$R_3 = \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix} \otimes \begin{bmatrix} 23 & 24 & 77 \\ 56 & 21 & 19 \\ 20 & 88 & 79 \end{bmatrix} \otimes \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix}$$
  $$R_3 = \begin{bmatrix} 56 & 21 & 19 \\ 20 & 88 & 79 \\ 23 & 24 & 77 \end{bmatrix}$$
  2) Compute the session key component
  $T_3 = P_{2,3} \otimes K_A \otimes Q_{2,3}$
  $$T_3 = \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix} \otimes \begin{bmatrix} 21 & 19 & 56 \\ 88 & 79 & 20 \\ 24 & 77 & 23 \end{bmatrix} \otimes \begin{bmatrix} 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \end{bmatrix}$$
  $$T_3 = \begin{bmatrix} 88 & 79 & 20 \\ 24 & 77 & 23 \\ 21 & 19 & 56 \end{bmatrix}$$
  3) Chipertext
  $S_3 = M + T$ *(element-wise addition)*
  $$S_3 = \begin{bmatrix} 65+88 & 48+79 & 48+20 \\ 48+24 & 48+77 & 48+23 \\ 48+21 & 48+19 & 48+56 \end{bmatrix}$$
  $$S_3 = \begin{bmatrix} 153 & 127 & 68 \\ 72 & 125 & 71 \\ 69 & 67 & 104 \end{bmatrix}$$

d) Transmission:
Send the pair *(S, R)* to Alice..

3. Decryption

a) Session key reconstruction
Alice Compute:

- Block 1
  $T_1 = P_1 \otimes R_1 \otimes Q_1$
  $$T_1 = \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix} \otimes \begin{bmatrix} 20 & 88 & 79 \\ 23 & 24 & 77 \\ 56 & 21 & 19 \end{bmatrix} \otimes \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix}$$
  $$T_1 = \begin{bmatrix} 24 & 77 & 23 \\ 21 & 19 & 56 \\ 88 & 79 & 20 \end{bmatrix}$$
- Block 2
  $T_2 = P_1 \otimes R_2 \otimes Q_1$
  $$T_2 = \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix} \otimes \begin{bmatrix} 24 & 77 & 23 \\ 21 & 19 & 56 \\ 88 & 79 & 20 \end{bmatrix} \otimes \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix}$$
  $$T_2 = \begin{bmatrix} 19 & 56 & 21 \\ 79 & 20 & 88 \\ 77 & 23 & 24 \end{bmatrix}$$
- Block 3
  $T_3 = P_1 \otimes R_3 \otimes Q_1$
  $$T_3 = \begin{bmatrix} -\infty & 0 & -\infty \\ -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \end{bmatrix} \otimes \begin{bmatrix} 56 & 21 & 19 \\ 20 & 88 & 79 \\ 23 & 24 & 77 \end{bmatrix} \otimes \begin{bmatrix} -\infty & -\infty & 0 \\ 0 & -\infty & -\infty \\ -\infty & 0 & -\infty \end{bmatrix}$$
  $$T_3 = \begin{bmatrix} 88 & 79 & 20 \\ 24 & 77 & 23 \\ 21 & 19 & 56 \end{bmatrix}$$

b) Plaintext recovery
Compute the original message block:

- Block 1
  $M_1 = S_1 - T_1$

$$M_1 = \begin{bmatrix} 89-24 & 152-77 & 108-23 \\ 53-21 & 102-19 & 141-56 \\ 163-88 & 144-79 & 52-20 \end{bmatrix}$$

$$M_1 = \begin{bmatrix} 65 & 75 & 85 \\ 32 & 83 & 85 \\ 75 & 65 & 32 \end{bmatrix}$$

- Block 2

$M_2 = S_2 - T_2$

$$M_2 = \begin{bmatrix} 96-19 & 121-56 & 105-21 \\ 148-79 & 97-20 & 153-88 \\ 161-77 & 96-23 & 99-24 \end{bmatrix}$$

$$M_2 = \begin{bmatrix} 77 & 65 & 84 \\ 69 & 77 & 65 \\ 84 & 73 & 75 \end{bmatrix}$$

- Block 3

$M_3 = S_3 - T_3$

$$M_3 = \begin{bmatrix} 153-88 & 127-79 & 68-20 \\ 72-34 & 125-77 & 71-23 \\ 69-21 & 67-19 & 104-56 \end{bmatrix}$$

$$M_3 = \begin{bmatrix} 65 & 48 & 48 \\ 48 & 48 & 48 \\ 48 & 48 & 48 \end{bmatrix}$$

c) Text Conversion

Convert the ASCII values of M back into characters.

$$M_1 = \begin{bmatrix} A & K & U \\ (space) & S & U \\ K & A & (space) \end{bmatrix}, M_2 = \begin{bmatrix} M & A & T \\ E & M & A \\ T & I & K \end{bmatrix}, M_3 = \begin{bmatrix} A & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Comparison

Table 1. Execution Time Comparison for Circulant Matrices

Case	Number of trials	Search time (s)	Results
Circulant 3 × 3	9	0,000808	Success
Circulant 4 × 4	16	0,003156	Success
Circulant 5 × 5	25	0,007090	Success
Circulant 8 × 8	100,000	55,619442	Failure
Circulant 9 × 9	100,000	98,586015	Failure
Circulant 10 × 10	100,000	106,213195	Failure

Table 2. Execution Time Comparison for Permutation Matrices

Case	Number of trials	Search time (s)	Results
Permutation 3 × 3	36	0.002061	Success
Permutation 4 × 4	576	0.092814	Success
Permutation 5 × 5	14400	4.207673	Success
Permutation 8 × 8	100,000	61.371280	Failure
Permutation 9 × 9	100,000	119.249227	Failure
Permutation 10 × 10	100,000	156.492677	Failure

Based on the experimental results presented in Tables 4.1 and 4.2, it can be concluded that the matrix size significantly affects the system's resistance to brute-force attacks. For small sizes 3⊗3 and 4⊗4, both circulant and permutation matrices remain vulnerable because the limited candidate space allows the key search to be completed in a very short time. When the size increases to 5⊗5,the execution time of the attack begins to rise, indicating an increase in computational complexity. The most noticeable differences are observed at sizes 8⊗8 to 10⊗10, where brute-force attacks are no longer successful even when the number of attempts is limited to 100,000, with execution times increasing drastically. This indicates that the larger the matrix dimension, the broader the candidate space that must be explored, thereby enhancing resistance to brute-force attacks. Furthermore, for

larger sizes, permutation matrices tend to require longer search times compared to circulant matrices, providing a slightly higher level of security.

CONCLUSIONS

Based on the discussion of the results, it can be concluded that this study successfully designed an encryption and decryption model for text messages based on the construction of permutation matrices in Max-Plus algebra, capable of consistently generating a shared secret key. Simulation results indicate that this model operates stably and accurately across various matrix sizes, while providing a higher level of security compared to the circulant matrix–based model. However, increasing the matrix size also leads to longer computation times, highlighting the need to balance security and efficiency in its implementation.

Future research is recommended to test the model with larger matrix sizes and to perform computational optimization to maintain efficiency. In addition, analyses of various types of cryptanalytic attacks should be conducted to evaluate the system's resilience. Implementing this model in real-time digital communication systems, as well as developing applications based on this algorithm, is also important to demonstrate its effectiveness and to broaden its application in the field of data security.

REFERENCES

Article, O. (2023). *CRYPTOGRAPHIC METHOD TO ENHANCE DATA SECURITY USING RSA ALGORITHM AND MELLIN TRANSFORM*. *7*(April), 63–72. https://doi.org/10.29121/IJOEST.v7.i2.2023.490

Durcheva, M. I. (2022). *TrES : Tropical Encryption Scheme Based on Double Key Exchange*. *2*(4), 11–17.

Huang, H., Li, C., & Deng, L. (2022). *applied sciences Public-Key Cryptography Based on Tropical Circular Matrices*. 1–12.

Muanalifah, A. (n.d.). *On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product arXiv : 2101 . 02781v3 [math . CO] 20 Sep 2021*.

Of, A., Protocols, F., On, B., & Matrices, C. (2023). *This preprint has not undergone peer review (when applicable) or any post-submission improvements or corrections . The Version of Record of this article is published in Indian Journal of Pure and Applied Mathematics , and is available online at*. 1–11.