ABSTRAK

Daniel Suleman, 2 0 2 5. *SISTEM KRIPTOGRAFI SUBSTITUSI-PERMUTASI ATAS ALJABAR MAX-PLUS*. **Skripsi.** Gorontalo. Program Studi Matematika. Jurusan Matematika. Fakultas Matematika dan Ilmu Pengetahuan Alam. Universitas Negeri Gorontalo.
Pembimbing : **(1) Nurwan, S.Pd., M.Si(2) Armayani Arsal, S.Si, M.Si**

Penelitian ini membahas perancangan dan evaluasi sistem kriptografi substitusi–permutasi berbasis aljabar Max-Plus sebagai alternatif pendekatan kriptografi modern yang efisien dan tahan terhadap serangan. Aljabar Max-Plus merupakan struktur semiring tropis dengan operasi utama maksimum $(\oplus)$ dan penjumlahan $(\otimes)$, yang memungkinkan pembentukan algoritma enkripsi non-linear. Proses enkripsi dilakukan dengan mengubah *plaintext* ke bentuk numerik menggunakan kode ASCII, kemudian dikonversi menjadi blok vektor dan diproses melalui operasi substitusi menggunakan matriks kunci diagonal berukuran 3×3 serta permutasi antar elemen blok dalam ruang Max-Plus. Proses dekripsi dilakukan dengan menggunakan invers dari matriks substitusi dan permutasi tersebut. Evaluasi keamanan dilakukan melalui analisis frekuensi dan simulasi serangan *brute force*, sedangkan efisiensi komputasi diukur berdasarkan waktu eksekusi dan penggunaan memori. Hasil penelitian menunjukkan bahwa sistem kriptografi berbasis Max-Plus mampu menghasilkan *ciphertext* dengan distribusi karakter yang acak, sulit ditebak, serta memiliki tingkat keamanan yang tinggi terhadap serangan analisis sederhana. Selain itu, pengujian performa memperlihatkan bahwa algoritma ini efisien dalam komputasi dengan waktu eksekusi yang meningkat secara linier terhadap panjang *plaintext* dan penggunaan memori yang stabil. Dengan demikian, sistem substitusi–permutasi atas aljabar Max-Plus berpotensi menjadi pendekatan alternatif yang aman dan efisien dalam pengembangan kriptografi modern.

Kata Kunci: *Kriptografi, Substitusi–Permutasi, Aljabar Max-Plus, Analisis Frekuensi, Brute Force, Efisiensi Komputasi.*

ABSTRACT

Daniel Suleman, 2025. *A SUBSTITUTION-PERMUTATION CRYPTOGRAPHIC SYSTEM OVER MAX-PLUS ALGEBRA.* **Undergraduate Thesis**. Gorontalo. Study Program of Mathematics, Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Negeri Gorontalo.
The Supervisors: **(1) Nurwan, S.Pd., M.Si., (2) Armayani Arsal, S.Si., M.Si.**

This study examined the design and evaluation of a substitution-permutation cryptographic system based on Max-Plus algebra as an alternative approach to modern cryptography, offering both efficiency and resistance to attacks. Max-Plus algebra is a tropical semiring structure characterized by the primary operations of maximum ($\oplus$) and addition ($\otimes$), which enables the construction of nonlinear encryption algorithms. The encryption process in this study was carried out by converting plaintext into numerical form using ASCII codes, which were then transformed into vector blocks and processed through substitution operations using a 3×3 diagonal key matrices, followed by permutations among block elements within the Max-Plus space. The decryption process used the inverse of the corresponding substitution and permutation matrices. Further, security evaluation was conducted through frequency analysis and brute-force attack simulations, while computational efficiency was assessed based on execution time and memory usage. The results indicated that the Max-Plus-based cryptographic system produced ciphertext with a random and unpredictable character distribution, demonstrating a high level of resistance to basic analytical attacks. Moreover, performance testing showed that the algorithm was computationally efficient, with execution time increasing linearly with plaintext length and stable memory consumption. Therefore, the substitution-permutation system over Max-Plus algebra represents a promising, secure, and efficient alternative approach for developing modern cryptographic schemes.

Keywords: *Cryptography, Substitution-Permutation, Max-Plus Algebra, Frequency Analysis, Brute-Force Attack, Computational Efficiency.*

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi yang berjudul **"SISTEM KRIPTOGRAFI SUBTITUSI-PERMUTASI ATAS ALJABAR MAX-PLUS"**

Oleh

DANIEL SULEMAN
NIM. 412421021

Telah diperiksa dan disetujui untuk diuji

Pembimbing I	Pembimbing II,
Nurwan, S.Pd., M.Si	**Armayani Arsal, S.Si, M.Si**
NIP. 198105102006041002	NIP. 199505142022032016

Mengetahui,
Koordinator Program Studi Matematika

Nisky Imansyah Yahya, S.Pd, M.Si
NIP.199107302020121008

LEMBAR PENGESAHAN

Skripsi yang berjudul **"SISTEM KRIPTOGRAFI SUBSTITUSI-PERMUTASI ATAS ALJABAR MAX-PLUS"**

Oleh

DANIEL SULEMAN
NIM. 412421021

Program Studi Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam

Telah dipertahankan di depan dewan penguji

Hari, tanggal	:	**Jumat, 31 Oktober 2025**
Waktu	:	**11.00-12.30 WITA**
Tempat	:	**Ruang Sidang Matematika**

	Pembimbing	**Tanda Tangan**
Pembimbing 1	**Nurwan, S.Pd., M.Si**	
	NIP. 198105102006041002	(.....)
Pembimbing 2	**Armayani Arsal, S.Si, M.Si**	
	NIP. 199505142022032016	(.....)
	Penguji	
Penguji 1	**Dr. Hasan S. Panigoro, S.Pd., M.Si**	
	NIP. 198910282020121015	(.....)
Penguji 2	**Asriadi, S.Pd., M.Si**	
	NIP. 198505012008121004	(.....)

Mengetahui,
Dekan Fakultas Matematika dan IPA

Prof. Dr. Fitryane Lihawa, M.Si
NIP. 196912091993032001