JIKTEKS : Jurnal Ilmu Komputer dan Teknologi Informasi
Vol. 03, No. 03, Agustus 2025, hlm. 25 - 29
ISSN : 2986-5417
DOI : doi.org/10.70404/jikteks.v3i03.322
Laman Jurnal: jurnal.faatuatua.com/index.php/JIKTEKS

Implementasi Algoritma Myszkowski Transposition Cipher Dalam Mengamankan Dokumen

Aliya Libya Pebriani
Informatika, Universitas Satya Terra Bhinneka, Indonesia
e-mail: *aliyapebriani@gmail.com*

Keywords:

First Keyword,
Second Keyword,
Third Keyword,
Fourth Keyword,
Fifth Keyword,

ABSTRACT

The abstract must be informative and clear which gives a statement about the background of the problem, the purpose of the study, the approach or method used, and shows the main findings and conclusions. Abstract written in one paragraph without a new paragraph with a number of words between 100 to 200 words. (9pt, Times New Roman).

Kata Kunci:

Kriptografi,
Enkripsi,
Dokumen Digital,
Myszkowski Cipher,
Keamanan Informasi.

ABSTRAK

Keamanan informasi digital menjadi kebutuhan penting di era pertukaran data yang semakin masif. Salah satu pendekatan yang dapat digunakan adalah kriptografi klasik dengan algoritma transposisi. Penelitian ini mengimplementasikan Myszkowski Transposition Cipher sebagai metode utama untuk mengamankan dokumen digital berformat .docx. Algoritma ini dipilih karena kemampuannya dalam menangani kunci dengan karakter berulang, sehingga menghasilkan pola enkripsi yang lebih kompleks dibandingkan transposisi sederhana. Proses penelitian meliputi perancangan sistem enkripsi-dekripsi, penerapan pada file dokumen, serta pengujian melalui black-box testing dan analisis kuantitatif terhadap waktu komputasi berdasarkan variasi ukuran dokumen. Hasil implementasi menunjukkan bahwa algoritma mampu menghasilkan ciphertext yang sulit dipecahkan tanpa kunci, serta mendemonstrasikan efisiensi waktu yang layak digunakan pada dokumen berukuran kecil hingga menengah. Kesimpulannya, Myszkowski Transposition Cipher dapat diandalkan sebagai algoritma standalone untuk pengamanan dokumen, sekaligus memberi dasar empiris bagi penelitian lanjutan mengenai integrasi cipher ini dalam skema super-encryption.

Korespondensi Penulis *):

Aliya Libya Pebriani
Universitas Satya Terra Bhinneka
Kota Medan, Provinsi Sumatera Utara.

Diajukan: 10-07-2025 | Diterima: 20-08-2025 | Diterbitkan: 30-08-2025

1. PENDAHULUAN

Dalam lingkup teknologi informasi kontemporer, keamanan informasi telah menjadi pilar utama kelangsungan operasional bisnis, pemerintahan, dan komunikasi personal [1]. Pertukaran dokumen digital, surat elektronik, dan data sensitif lainnya melalui jaringan terbuka seperti internet terus meningkat secara eksponensial [2]. Kondisi ini menciptakan celah kerentanan yang signifikan terhadap ancaman siber, penyadapan (eavesdropping), dan modifikasi data oleh pihak yang tidak berhak [3]. Oleh karena itu, kebutuhan akan mekanisme perlindungan data yang efektif dan efisien menjadi sangat mendesak.

Kriptografi adalah disiplin ilmu yang mempelajari teknik penyandian pesan untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan autentikasi data [4]. Secara historis, kriptografi terbagi menjadi dua kategori besar: kriptografi modern (seperti AES dan RSA) dan kriptografi klasik. Kriptografi klasik, meskipun sederhana dari segi komputasi, menawarkan dasar teoritis yang kuat melalui dua teknik dasar: substitusi (penggantian karakter) dan transposisi (pengubahan posisi karakter) [5].

Penelitian ini berfokus pada salah satu algoritma klasik jenis transposisi, yaitu Myszkowski Transposition Cipher. Algoritma yang diperkenalkan oleh Émile Victor Théodore Myszkowski pada tahun 1902 ini merupakan varian lanjutan dari Columnar Transposition Cipher [6]. Keunikan Myszkowski terletak pada cara penanganan kunci

yang memiliki huruf berulang (repeating letters), di mana kolom-kolom dengan nomor kunci yang sama dibaca secara horizontal baris per baris, bukan secara vertikal per kolom [7]. Kompleksitas pembacaan inilah yang membuat cipher ini memiliki tingkat kesulitan pemecahan yang lebih tinggi dibandingkan transposisi sederhana, menjadikannya menarik untuk diimplementasikan dalam pengamanan dokumen digital [8].

Telah banyak penelitian yang mengimplementasikan kriptografi klasik, baik secara tunggal maupun hibrida. Misalnya, kombinasi Affine Cipher dan Myszkowski Transposition telah terbukti meningkatkan keamanan pesan pada aplikasi instant messaging dengan waktu komputasi yang terukur [9]. Selain itu, algoritma ini juga digunakan dalam skema super encryption untuk pengamanan citra digital [10]. Namun, implementasi spesifik Myszkowski Transposition Cipher sebagai algoritma utama untuk mengamankan keseluruhan dokumen teks dengan menguji pure performance enkripsi dan dekripsinya, serta menganalisis efektivitas pengamanan dalam konteks dokumen (bukan hanya pesan singkat), masih memerlukan studi mendalam [11], [12].

Berdasarkan latar belakang tersebut, permasalahan yang akan dipecahkan dalam penelitian ini adalah: Bagaimana merancang dan mengimplementasikan algoritma Myszkowski Transposition Cipher ke dalam sebuah aplikasi yang mampu melakukan proses enkripsi dan dekripsi secara fungsional pada dokumen digital berekstensi teks? Kemudian bagaimana menganalisis dan mengukur kinerja waktu komputasi (running time) yang dibutuhkan oleh algoritma Myszkowski Transposition Cipher dalam proses enkripsi dan dekripsi berdasarkan variasi ukuran dokumen yang berbeda?

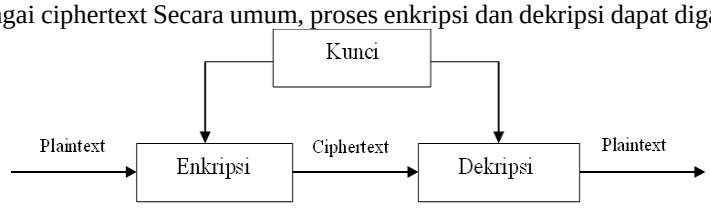
Sejalan dengan permasalahan di atas, tujuan penelitian ini adalah: Mengimplementasikan algoritma Myszkowski Transposition Cipher pada platform pengembangan untuk menghasilkan ciphertext dan mengembalikannya menjadi plaintext pada dokumen. Melakukan pengujian fungsionalitas (black-box testing) dan menganalisis secara kuantitatif waktu komputasi algoritma sebagai dasar evaluasi efisiensi sistem dalam mengamankan dokumen.

Penelitian ini diharapkan dapat memberikan inovasi riset berupa dokumentasi implementasi praktis Myszkowski Transposition Cipher sebagai standalone cipher untuk dokumen, serta menyediakan data empiris mengenai efisiensi kinerja running time algoritma tersebut sebagai referensi perbandingan bagi pengembangan skema super-encryption di masa depan [13], [14], [15].

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Kriptografi sendiri menggunakan teknik matematika untuk mengacak pesan dan membuatnya tidak dapat terbaca oleh pihak yang tidak berhak. Kriptografi memiliki dua konsep penting yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi yang akan dikirim diubah menjadi bentuk yang hampir tidak dikenali. Dekripsi adalah proses mengubah kembali bentuk tidak dikenali menjadi informasi awal. Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah plaintext. Kemudian setelah disamarkan dengan suatu cara penyandian, maka plaintext ini disebut sebagai ciphertext Secara umum, proses enkripsi dan dekripsi dapat digambarkan sebagai berikut:



Gambar 1. Skema Proses Enkripsi Dan Dekripsi

Pada Gambar 1 ditunjukkan skema proses enkripsi dan dekripsi. Dimana pada proses enkripsi, dapat dilihat bahwa plaintext akan dienkripsikan sehingga menghasilkan keluaran berupa ciphertext, dimana ketika ciphertext didekripsikan akan menghasilkan plaintext

2.2 Myszkowski Transposition Cipher

Algoritma *Myszkowski Transposition Cipher* merupakan salah satu jenis algoritma tranposisi cipher yang memiliki keunikan tersendiri. Pada proses enkripsi, plaintext ditulis secara horizontal dari kiri ke kanan, kemudian ciphertext dibaca secara vertikal sesuai dengan urutan kunci dan pada proses dekripsi dapat dilakukan apabila pihak penerima pesan rahasia (ciphertext) mengetahui pola kunci dan ukuran baris dan kolom yang digunakan pihak pengirim pesan. Myszkowski Transposition untuk kedepannya ditulis dalam matriks secara rowwise manner. Enkripsi ini merupakan variasi dari columnar transposition. Myszkowski Transposition merupakan algoritma yang mirip dengan columnar transposition, hanya saja algoritma ini menggunakan key dari karakter berulang[9]. Contoh : Key LAPTOP mempunyai urutan [2 1 4 6 3 5]. Kolom plainteks dengan nomor urutan angka yang unik dibaca kebawah, sedangkan yang sama dibaca dari kiri ke kanan. Plainteks : SAYA KULIAH DI BUDIDARMA key = [2 1 4 5 3 4].

Tabel 1. Kolom Pengurutan Proses Enkripsi

L	A	P	T	O	P

2	**1**	**4**	**5**	**3**	**4**
S	A	Y	A	K	U
L	I	A	H	D	I
B	U	D	I	D	A
R	M	A			

Maka diperoleh hasil cipertext: AIUM SLBR KDD YUAIDAA AHI.

2.3 File Dokumen

Dokumen adalah warkat asli yang dipergunakan sebagai alat pembuktian atau sebagai bahan untuk mendukung suatu keterangan. Dokumen dalam kamus komputer bisa dikatakan file yang dibuat oleh software, misalnya seperti Ms word coreldraw notepad dan masih banyak lainya. Sementara istilah "dokumen" pada awalnya disebut khusus untuk dokumen pengolah kata, sekarang digunakan untuk merujuk ke semua jenis file yang disimpan. Oleh karena itu, dokumen dapat berisi teks, gambar, audio, video, dan tipe data lainnya. Sebagian besar nama file dokumen juga menyertakan ekstensi file yang menentukan jenis file dokumen. Misalnya, dokumen Microsoft Word memiliki ekstensi file *docx, sedangkan dokumen Photoshop memiliki ekstensi file .PSD[8].

3. HASIL DAN ANALISIS

3.1 Analisa

Dalam hal ini peneliti menerapkan algoritma Myszkwoski Transposition Chiper untuk mengamankan file dokumen dengan dilakukan proses enkripsi agar file yang telah dienkripsi diubah lagi nilai bitnya sehingga mempersulit pihak lain yang ingin mengetahui isi dari file dokumen tersebut.

Algoritma Myszkowski Transposition Cipher merupakan salah satu jenis algoritma tranposisi cipher yang memiliki keunikan tersendiri. Pada proses enkripsi, plaintext ditulis secara horizontal dari kiri ke kanan, kemudian ciphertext dibaca secara vertikal sesuai dengan urutan kunci dan pada proses dekripsi dapat dilakukan apabila pihak penerima pesan rahasia (ciphertext) mengetahui pola kunci dan ukuran baris dan kolom yang digunakan pihak pengirim pesan. Keamanan dokumen dilakukan dengan cara menyandikan dokumen asli menjadi dokumen yang sulit untuk dimengerti, dan hanya bisa diakses oleh pihak yang memiliki sandi atau kuncinya. File dokumen yang akan dienkripsi berformat *.docx dengan menerapkan algoritma Myszkwoski Transposition Chiper, setelah file dokumen dienkripsi.

3.2 Penerapan Algoritma Myszkowski Transposition Cipher

Langkah 1: Menyiapkan Kunci dan Menentukan Urutan Kolom
Misalkan kita menggunakan kunci: "DOCUMENT"
Kita beri nomor urut berdasarkan urutan abjad dari kunci:
D O C U M E N T
2 5 1 7 4 3 6 8

Penjelasan:
Huruf C paling kecil → urutan 1
D → urutan 2
E → urutan 3
M → urutan 4
O → urutan 5
N → urutan 6
U → urutan 7
T → urutan 8

Langkah 2: Menyusun Data dalam Matriks Berdasarkan Kunci
Data hex yang diberikan:
50 4B 03 04 14 00 06 00 08 00 00 00 21 00 2F B2
A8 74 81 01 00 00 D9 05 00 00 13 00 08 02 5B 43

Kita ubah ke bentuk desimal (dalam bentuk byte):
80 75 3 4 20 0 6 0 8 0 0 0 33 0 47 178
168 116 129 1 0 0 217 5 0 0 19 0 8 2 91 67
Kita susun dalam matriks dengan kolom sesuai urutan kunci di atas.
Jumlah kolom = 8 (sesuai panjang kunci)

Jumlah baris = total data / 8 = 32 / 8 = 4 baris.
Tabel penempatan (dalam desimal):

Kolom Urut Kunci	2 (D)	5 (O)	1 (C)	7 (U)	4 (M)	3 (E)	6 (N)	8 (T)
Baris 1	80	20	3	0	4	0	8	0
Baris 2	0	33	0	47	178	168	116	129
Baris 3	1	0	0	217	5	0	0	19
Baris 4	0	8	2	91	67			

Langkah 3: Membaca Ciphertext Berdasarkan Aturan Myszkowski
Aturan Myszkowski:
Kolom dengan nomor urut unik dibaca dari atas ke bawah.
Kolom dengan nomor urut sama (tidak terjadi di sini) dibaca dari kiri ke kanan per baris.
Urutan baca berdasarkan nomor urut terkecil ke terbesar:
1, 2, 3, 4, 5, 6, 7, 8

Kolom 1 (C):
3, 0, 0, 2
→ 3 0 0 2

Kolom 2 (D):
80, 0, 1, 0
→ 80 0 1 0

Kolom 3 (E):
0, 168, 0
→ 0 168 0

Kolom 4 (M):
4, 178, 5, 67
→ 4 178 5 67

Kolom 5 (O):
20, 33, 0, 8
→ 20 33 0 8

Kolom 6 (N):
8, 116, 0
→ 8 116 0

Kolom 7 (U):
0, 47, 217, 91
→ 0 47 217 91

Kolom 8 (T):
0, 129, 19
→ 0 129 19

Langkah 4: Gabungkan Semua Bagian
Ciphertext (dalam desimal):

3 0 0 2 80 0 1 0 0 168 0 4 178 5 67 20 33 0 8 8 116 0 0 47 217 91 0 129 19

Hasil Akhir Enkripsi Myszkowski
Plaintext (desimal):
80 75 3 4 20 0 6 0 8 0 0 0 33 0 47 178 168 116 129 1 0 0 217 5 0 0 19 0 8 2 91 67

Ciphertext (desimal) setelah enkripsi Myszkowski:
3 0 0 2 80 0 1 0 0 168 0 4 178 5 67 20 33 0 8 8 116 0 0 47 217 91 0 129 19

4. KESIMPULAN

Kesimpulan menjelaskan jawaban dari apa yang diharapkan dari sebuah penelitian yang telah dijelaskan dibagian Pendahuluan. Pada bagian ini dapat ditambahkan saran untuk pengembangan penelitian selanjutnya berdasarkan hasil dan analisa yang telah dilakukan. Kesimpulan dapat berupa paragraf atau berupa poin-poin.

REFERENSI

[1] [1] N. S. H. Nurhaida and A. F. Harahap, "Penerapan Kriptografi Klasik untuk Keamanan Database Pada Badan Pengawasan Pemilu Kabupaten Seluma," Jurnal Sosial Sains (J-SOSSA), vol. 3, no. 5, pp. 4749–4757, 2023.
[2] [2] R. M. F. Lubis, H. S. Sembiring, and A. Albar, "Sistem Kriptografi pada Pengamanan Autentikasi Dokumen Elektronik: Systematic Literature Review," Khazanah: Jurnal Pengembangan Kearsipan, vol. 15, no. 2, pp. 116–129, 2022.
[3] [3] M. I. Prayoga, A. S. B. Nur, and A. H. H. Siregar, "Penggunaan Cryptography dalam Keamanan Pesan Digital," Jurnal of Computer Science and Information Technology (JOCSI), vol. 1, no. 1, pp. 10–18, 2024.
[4] S. A. A. A. Rahmat and S. F. P. Sari, "Penerapan Sistem Kriptografi Enkripsi Jamak dan Tanda Tangan Digital dalam Mendukung Keamanan Informasi," Tematika, vol. 11, no. 1, pp. 24–35, 2024.
[5] R. Munir, "Kriptografi Klasik," in Prodi Sistem dan Teknologi Informasi, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, 2021.
[6] J. T. Tarigan and F. Chairinnisa, "Combination of Myszkowski Transposition Algorithm and Modified Least Significant Bit (MLSB) Green Channel on PNG Image Security," Journal of Physics: Conference Series, vol. 1255, no. 1, p. 012017, 2019.
[7] V. N. T. D. R. Harahap and D. R. D. Damanik, "Penerapan Algoritma Myszkowski Transposition Cipher untuk Mengamankan Pesan Teks pada Aplikasi Chat," Jurnal Media Informatika Budidarma, vol. 7, no. 3, pp. 1827–1836, 2023.
[8] M. H. F. Pratama and I. Setiarso, "Implementasi Algoritma Base64 untuk Enkripsi dan Dekripsi Teks Menggunakan Bahasa Pemrograman Python," Jurnal Applied Intelligent System, vol. 4, no. 1, pp. 1–10, 2022.
[9] K. A. Harahap, M. S. Lydia, and Herriyance, "Implementasi Super Enkripsi dengan Algoritma Affine Cipher dan Myszkowski Transposition pada Instant Messaging," Undergraduate Theses, Repositori Universitas Sumatera Utara, 2023.
[10] E. Piona, A. Fauzi, and M. A. Syari, "Digital Image Security Implementation With Uses Super Encryption Algorithm Myszkowski And The Algorithm Paillier Cryptosystem," Journal of Artificial Intelligence and Computing, vol. 4, no. 2, pp. 129–137, 2022.
[11] N. K. Harahap and M. K. Harahap, "Modifikasi Myszkowski Transposition Cipher dengan Chess Board Pattern," Seminar Nasional Ilmu Komputer (SNASIKOM), pp. 1–6, 2019.
[12] H. S. M. Hardi and D. Rachmawati, "Enhancing Resistance of Hill Cipher using Columnar and Myszkowski Transposition," International Journal of Computer Sciences and Engineering, vol. 3, no. 1, pp. 31–36, 2015.
[13] M. Meylissa, Khairil, and J. Jumadi, "Implementasi Kombinasi Algoritma Myszkowski Transposition dan Vigenere Cipher pada Keamanan untuk File Teks," Seminar Nasional Ilmu Komputer (SNASIKOM), pp. 15–26, 2023.
[14] R. Yusuf, M. Hilmi, and H. Lestiawan, "Super Encryption Video Cryptography: Combination of Vigenere Cipher and Myszkowski Transposition," 2022 International Seminar on Application for Technology (ISAT), IEEE, pp. 123–128, 2022.
[15] B. Firmanto, "Perbandingan Hasil Performa Optimasi Transposisi Hill Cipher dan Vigenere Cipher pada Citra Digital," SMARTICS Journal, vol. 7, no. 2, pp. 65–71, 2021.