Journals.Telkomuniversity.ac.id

Journal of Software Engineering and Multimedia **(JASMED)**

Vol. 3 No. 2 (2025) | eISSN:3025-6372 |
https//doi.org/10.20895/jasmed.v3i2.10097

Full Paper

Combination of Rail Fence and Route Cipher: Dual Encryption Strategy in Digital Messages

Asih Lestari[1],
Tunas Pembangunan University Surakarta, Surakarta, Indonesia,
f0223004_asihlestari@student.utp.ac.id
Nanda Putri Tami[2],
Tunas Pembangunan University Surakarta, Surakarta, Indonesia
f0223007_nandaputritami@student.utp.ac.id
Fabianus Delan Saputra[3],
Tunas Pembangunan University Surakarta, Surakarta, Indonesia
f022002_fabianusdelansaputra@student.utp.ac.id
Erni Widarti[4*],
Tunas Pembangunan University Surakarta, Surakarta, Indonesia
erni.widarti@lecture.utp.ac.id

*Corresponding Author

ABSTRACT

In today's digital era, the protection of personal and sensitive information has become a critical challenge due to the rapid growth of cyber threats and unauthorized access. Encryption remains one of the most effective strategies to ensure confidentiality and integrity of digital communication. This study proposes a dual encryption approach by combining two classical transposition algorithms: Rail Fence Cipher and Route Cipher. The Rail Fence Cipher rearranges plaintext into a zig-zag pattern across multiple rails, producing an initial ciphertext that obscures the original structure. The Route Cipher then strengthens security by placing this ciphertext into a matrix and reading it according to a predefined route, such as spiral or zig-zag, thereby generating a second ciphertext with higher complexity. The combination of these methods creates layered encryption that is more resistant to cryptanalysis compared to using either algorithm alone. Experimental implementation using Python demonstrates that the dual encryption strategy produces ciphertext that is significantly more randomized and difficult to predict. While this approach does not guarantee absolute security against modern attacks, it offers a practical solution for small-scale applications, educational purposes, and scenarios requiring lightweight encryption. The findings encourage broader adoption of encryption techniques and highlight the relevance of classical algorithms in understanding fundamental cryptographic principles and developing adaptable security strategies in the evolving digital landscape.

KEYWORDS

Rail Fence; Route Cipher; Encryption; Digital Message Security

Lestari, A., Tami, N. P., Saputra, F. D., Widarti, E. (2025). Combination of Rail Fence and Route Cipher: Dual Encryption Strategy in Digital Messages. jasmed, 3(2), pp. 75-85. https//doi.org/10.20895/jasmed.v3i2.10097

Article Submitted 06/11/20245. Revision uploaded 24/12/2025. Accepted 24/12/2025.

1. INTRODUCTION

Pesatnya perkembangan teknologi informasi menjadikan informasi sebagai kebutuhan pokok bagi setiap orang. Seiring berkembangnya teknologi, maka keamanan terhadap kerahasiaan data dan informasi yang dipertukar akan semakin meningkat [1]. Keamanan data diperlukan agar meminimalkan pencurian data. Untuk mencapai keamanan data tersebut, dilakukan proses penyandian terhadap data tersebut [2]. Salah satu teknik dasar yang banyak digunakan dalam menjaga keamanan data adalah melalui kriptografi teknik transposisi [3]. Oleh karena itu dengan adanya jurnal ini dibuat bagi pembaca supaya bisa mengamankan keamanan data personal mereka secepatnya di era kemajuan teknologi semakin pesat. Salah satu solusi untuk mengamankan data adalah dengan menggunakan kriptografi [4]. Kriptografi berperan penting dalam menjaga keamanan data dengan mempelajari berbagai teknik yang bertujuan untuk mengamankan sebuah informasi dengan mengacak informasi tersebut sehingga tidak dapat dipahami oleh pihak yang tidak berwenang [5]. Kriptografi ialah ilmu yang menekuni bagaimana melaksanakan enkripsi serta dekripsi, dengan menggunakan model matematika tertentu [6]. Proses pengubahan plaintext menjadi ciphertext disebut sebagai enkripsi (encryption), sedangkan proses pengembaliannya disebut sebagai dekripsi (decryption), Ilmu kriptografi terletak pada proses logika saat untuk proses enkripsi dan dekripsi dimana proses tersebut sebaiknya dibuktikan bukan hanya sekedar teoritis saja [7]. Sehingga parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan. Kriptografi fokus pada keamanan kunci, bukan algoritma [8].

Perlindungan pesan digital menjadi semakin penting di era saat ini, di mana data dan informasi digital sering menjadi ancaman oleh pihak yang tidak bertanggung jawab [9]. Ancaman terhadap privasi dan integritas informasi tidak hanya datang dari pihak internal, tetapi juga dari individu, kelompok, bahkan negara yang berupaya mengakses data sensitif tanpa otorisasi. Dalam konteks ini, pemeriksaan terhadap keamanan sistem dan perlindungan data pribadi masyarakat menjadi sangat penting untuk mencegah potensi penyalahgunaan maupun pelanggaran privasi [10]. Karena itulah, pentingnya mengembangkan strategi dan teknologi yang dapat melindungi data, agar keamanan komunikasi digital tetap terjaga [11]. Oleh karena itu, menjaga keutuhan dan kerahasiaan data pribadi menjadi aspek krusial yang harus diberikan perhatian serius dalam upaya mencegah kerugian yang berpotensial timbul [12]. Penelitian ini bertujuan untuk mengusulkan kombinasi teknik enkripsi Rail fense dan Route cipher sebagai strategi enkripsi ganda guna meningkatkan keamanan pesan digital. Dengan semakin tingginya kebutuhan akan proteksi data dalam komunikasi digital, teknik enkripsi ganda diharapkan dapat menawarkan tingkat perlindungan yang lebih kuat terhadap ancaman seperti pencurian data dan akses ilegal. Dari penelitian ini menggabungkan kedua algoritma klasik tersebut untuk mempersulit dekripsi oleh pihak yang tidak berwenang. Harapannya, kombinasi ini dapat menjadi solusi praktis dalam menjaga kerahasiaan informasi digital dan mendorong penerapan enkripsi yang lebih luas dalam berbagai aplikasi keamanan siber.

Kriptografi merupakan teknik penyandian pesan secara tersembunyi dengan menggunakan kode-kode untuk mengamankan informasi dengan tujuan utama menjaga kerahasiaan, integritas, dan keabsahan data. Kriptografi bekerja dengan cara mengacak teks biasa menjadi teks sandi sehingga hanya penerima yang dituju yang dapat memahaminya. Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata kriptografi dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti secret (rahasia), graphia berarti writing (tulisan). Kriptografi memiliki sejarah yang sangat menarik dan panjang. Kriptografi sudah digunakan 4000 tahun yang lalu dan diperkenalkan oleh orang-orang Mesir untuk mengirim pesan ke pasukan militer yang berada dilapangan [13]. Kriptografi yang memiliki peran untuk menyimpan suatu pesan informasi kedalam media tertentu agar pesan yang tersimpan tidak mudah diketahui keberadaan sekaligus dengan mata penglihatan manusia [14]. Sandi Rail fense Cipher atau dapat disebut sebagai sandi pagar rel adalah teknik penyandian yang mengacak urutan huruf dalam suatu pesan dengan cara menuliskan pesan secara zig zag pada baris-baris bergantian di atas kertas. Asal muasal sandi Rail Fense tidak diketahui secara pasti, tetapi diyakini telah digunakan oleh orang Yunani dan Sparta kuno sebagai metode komunikasi rahasia. Sandi Rail Fense semakin mendapat perhatian selama Perang Saudara Amerika pada tahun 1860-an, yang digunakan untuk menyembunyikan pesan militer Union maupun mata-mata konfederasi [2]. Sedangkan ciphertext-nya diperoleh dengan membaca huruf berdasarkan baris [15].

Route Cipher adalah sebuah teknik kriptografi klasik yang menggunakan transposisi untuk melakukan enkripsi. Pada metode ini, teks plaintext awalnya ditulis dalam grid dengan dimensi tertentu, dan kemudian dibaca berdasarkan pola yang ditentukan oleh kunci. Untuk pesan yang panjang, jumlah kemungkinan kunci bisa menjadi sangat besar sehingga sulit untuk dihitung, penting untuk diingat bahwa semua kunci memiliki tingkat keamanan yang

sama [16]. Algoritma route cipher dapat dikatakan mempunyai proses enkripsi yang rumit. Hal tersebut dikarenakan key atau kunci yang lebih membuat proses enkripsi dan dekripsi menjadi fleksibel. Bila panjang karakter tidak habis dibagi dengan panjang karakter, maka penambahan karakter secara dummy saat melakukan enkripsi [17]. Secara sederhana dalam proses enkripsi transposisi route cipher, pesan asli dipecah menjadi bagian-bagian kecil yang kemudian diatur ulang atau ditransposisikan sesuai dengan rute yang telah ditentukan, sehingga menghasilkan teks sandi yang membingungkan [18].

Pada penelitian kali ini akan dilakukan penggabungan dua algoritma kriptografi untuk membangun enkripsi ganda menggunakan algoritma Rail Fense Cipher dan Route Cipher dalam mengamankan pesan. Kombinasi ini memanfaatkan kekuatan masing-masing metode transposisi untuk meningkatkan kompleksitas dalam penyusunan pesan, sehingga lebih sulit untuk dipecahkan tanpa kunci yang tepat. Dalam dunia modern, meskipun algoritma kriptografi modern seperti AES (Advanced Encryption Standard) dan RSA (Rivest-Shamir-Adleman) menjadi standar untuk pengamanan data, studi terhadap enkripsi klasik seperti Rail Fense dan Route Cipher masih relevan untuk memahami prinsip dasar transposisi, terutama dalam pengajaran dasar-dasar kriptografi serta aplikasi pada data berukuran kecil atau pesan tertentu.

Penelitian ini mengenai kombinasi algoritma kriptografi rail fense cipher dan route cipher, pengamanan basis data, implementasi algoritma, analisis performansi kriptografi. Penelitian yang berjudul "Kombinasi Algoritma Kriptografi Transposisi Rail Fense Cipher dan Route Cipher" bertujuan untuk mengetahui seberapa persen tingkat keamanan pesan yang dihasilkan. Dengan hasil kombinasi Rail Fense Cipher dan Route Cipher menghasilkan cipherteks yang lebih rumit dan sulit dipecahkan. Menggunakan pengujian terhadap 13 karakter plainteks, tingkat kekuatan cipherteks yang dihasilkan mencapai 52%, sedangkan saat pengujian terhadap 23 karakter plainteks, tingkat kekuatan cipherteks mencapai 100%. Kekurangan dari penelitian ini adalah tidak membahas mengenai kecepatan suatu algoritma, sehingga penting untuk mempertimbangkan waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi, terutama untuk aplikasi yang memerlukan performa tinggi [2].

Penelitian yang berjudul "Pengamanan Basis data Dengan Algoritma Transposisi Rail Fense" Penelitian ini bertujuan untuk menginvestigasi penggunaan salah satu algoritma dalam kriptografi, yaitu transposisi Rail Fense dalam mengamankan data pemasok. Dengan hasil penelitian menunjukkan bahwa penggunaan metode Rail Fense dapat diterapkan untuk meningkatkan keamanan data pemasok dalam sebuah perusahaan. Kekurangan penelitian ini adalah tidak menutup kemungkinan tetap ada celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab [3]. Penelitian yang berjudul "Implementasi Algoritma One Time menggunakan Algoritma Cipher Transposition Sebagai pengaman Rahasia Pesan Rail Fense Cipher Dan Route Cipher Untuk Keamanan File" penelitian ini bertujuan untuk menjaga kerahasiaan dalam pemakaiannya sehingga sangat penting dalam enkripsi dan dekripsi dan Penggunaan pemisah kata (spasi) pada proses enkripsi sangat berpengaruh terhadap pembentukan karakter matriks sehingga menghasilkan plainteks yang sesuai dengan pesan aslinya. Algoritma One Time Pad (OTP) merupakan stream cipher yang melakukan enkripsi & dekripsi satu karakter setiap kali. Algoritma One Time Pad memiliki kriteria panjang teks sama dengan panjang key jika tidak sama maka karakter pesan pada key akan melakukan iterasi pesan dan panjang pesan sama dengan panjang key. Algoritma One Time Pad aman dipakai dalam penyandian, karena memiliki key yang berbeda di setiap penyandiannya terhadap pesan asli, algoritma ini memiliki kelemahan pada dekripsinya yang terkadang cipherteks tidak dapat kembali secara utuh [9].

Penelitian yang berjudul "Implementasi Algoritma Super Enkripsi Vigenere Cipher Dan Route Cipher Pada Penyandian Pesan Teks" penelitian ini bertujuan untuk mengimplementasikan algoritma super enkripsi Vigenere Cipher dan Route Cipher pada penyandian pesan teks. Hasil penelitian menunjukkan bahwa metode enkripsi gabungan ini mampu meningkatkan tingkat keamanan pesan dibandingkan dengan menggunakan salah satu algoritma saja. Kelemahan utama dari metode enkripsi gabungan Vigenere Cipher dan Route Cipher terletak pada kompleksitas implementasi yang berpotensi menimbulkan kesalahan dan penurunan efisiensi. Selain itu, analisis kriptografi yang belum mendalam membuat kekuatan sebenarnya dari metode ini masih dipertanyakan dan rentan terhadap berbagai jenis serangan. Terbatasnya panjang kunci juga menjadi kendala, karena kunci yang terlalu pendek dapat memudahkan serangan brute-force. Untuk mengatasi hal ini, perlu dilakukan optimasi algoritma, analisis kriptografi yang lebih komprehensif, dan penggunaan panjang kunci yang cukup kuat [11].

Penelitian yang berjudul "Analisis Performansi Kriptografi Berbasis Algoritma Caesar Cipher dan Rail Fense Cipher pada Tembang Macapat" penelitian ini bertujuan untuk membandingkan algoritma Caesar Cipher dan Rail Fense Cipher untuk mengetahui proses penyandian dan efektifitas waktu enkripsi dan deskripsi. Hasil menunjukkan waktu deskripsi lebih lama dibandingkan enkripsi. Waktu rata-rata enkripsi algoritma Rail Fense Cipher lebih cepat yaitu

adalah 0.000254 detik dibandingkan dengan Caesar. Waktu rata-rata enkripsi Rail Fense Cipher adalah 0.000254 detik dan waktu deskripsi adalah 0.000475 detik. Waktu enkripsi terpendek Pocung dan Kinanti. Rail Fense lebih aman di banding Caesar Cipher. Kekurangan dari penelitian ini masih sebatas proses penerapan enkripsi dan deskripsi terhadap plaintext yang digunakan, dengan adanya keterbatasan dalam pengujian yang lebih efektif [19]. Fokus penelitian ini adalah kombinasi algoritma Rail Fense Cipher dan Route Cipher, yang dapat meningkatkan keamanan pesan dan waktu enkripsi. Sehingga mudah untuk diimplementasikan pada aplikasi sederhana. Selain itu, metode enkripsi ganda kombinasi Rail Fense Cipher dan Route Cipher menawarkan metode yang lebih sederhana namun aman.

2. METHODS

Metode dalam penelitian ini menggabungkan dua algoritma kriptografi klasik, yaitu *Rail Fence Cipher* dan *Route Cipher*, untuk menghasilkan lapisan keamanan yang lebih kuat dalam proses penyandian data. Kombinasi kedua algoritma ini diharapkan dapat meningkatkan tingkat kompleksitas enkripsi sehingga lebih sulit untuk dianalisis atau dipecahkan oleh pihak yang tidak berwenang, terutama dalam konteks serangan kriptanalisis. Dengan menggabungkan dua metode transposisi yang berbeda prinsip dan pola pengacakannya, sistem enkripsi ini berupaya menciptakan hasil *ciphertext* yang memiliki distribusi karakter acak dan sulit ditebak, sekaligus mempertahankan efisiensi proses enkripsi dan dekripsi.

Rail Fence Cipher dipilih sebagai lapisan pertama dalam proses enkripsi karena algoritma ini mampu mengubah susunan karakter *plaintext* ke dalam pola zig-zag berdasarkan jumlah rel atau tingkat yang ditentukan oleh kunci. Sementara itu, *Route Cipher* berperan sebagai lapisan kedua yang memperkuat keamanan dengan menambahkan pola pembacaan karakter berdasarkan arah atau rute tertentu di dalam matriks yang terbentuk dari hasil enkripsi tahap pertama. Kombinasi kedua algoritma ini dirancang untuk saling melengkapi: *Rail Fence Cipher* memberikan efek pengacakan linear vertikal-horizontal, sedangkan *Route Cipher* menambahkan kompleksitas spasial melalui pola pembacaan multidimensi. Secara umum, alur proses kombinasi kedua algoritma ini dapat dilihat pada **Figure 1**, yang menjelaskan tahapan penyandian data dari *plaintext* hingga menjadi *ciphertext* akhir yang telah dienkripsi secara berlapis.

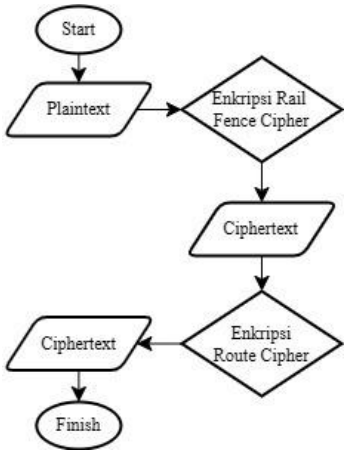

Figure 1 Alur proses kombinasi *rail fence* dan *route cipher*

Tahapan pertama dalam proses enkripsi adalah penerapan *Rail Fence Cipher*. Algoritma ini bekerja dengan cara mengatur karakter *plaintext* ke dalam pola zig-zag pada sejumlah rel tertentu yang ditentukan berdasarkan kunci yang digunakan. Misalnya, jika kunci yang digunakan adalah angka 3, maka karakter *plaintext* akan disusun ke dalam 3 rel. Proses penulisan karakter dilakukan dengan pola turun ke bawah lalu naik kembali ke atas secara berulang hingga semua karakter *plaintext* terisi ke dalam pola tersebut. Setelah karakter disusun dalam bentuk zig-zag, maka hasil enkripsi tahap pertama diperoleh dengan membaca karakter dari rel pertama ke rel terakhir, yaitu secara berurutan dari atas ke bawah. Dengan demikian, teks yang dihasilkan dari proses *Rail Fence Cipher* bukan lagi menyerupai bentuk asli dari pesan awal, melainkan telah mengalami pengacakan posisi karakter. Hasil sementara inilah yang selanjutnya akan menjadi input untuk tahap kedua, yaitu proses *Route Cipher*. *Rail Fence Cipher* digunakan dalam tahap pertama karena kemampuannya untuk menghasilkan perubahan posisi karakter yang cukup signifikan dengan

cara sederhana dan cepat. Meskipun algoritma ini termasuk jenis *cipher* klasik yang relatif mudah dipahami, namun ketika dikombinasikan dengan algoritma lain, tingkat keamanan yang dihasilkan meningkat secara signifikan.

Tahapan kedua dalam penelitian ini adalah penerapan *Route Cipher* terhadap hasil enkripsi sementara dari tahap sebelumnya. Pada tahap ini, teks hasil *Rail Fence Cipher* akan dimasukkan ke dalam suatu matriks persegi panjang sesuai dengan panjang kunci atau ukuran grid yang telah ditentukan. Misalnya, jika kunci yang digunakan adalah 4x4, maka karakter hasil enkripsi sementara akan diisi ke dalam matriks tersebut secara berurutan. Setelah seluruh karakter ditempatkan dalam matriks, proses pembacaan dilakukan berdasarkan pola rute tertentu. Pola ini bisa berupa spiral (memutar dari luar ke dalam), zig-zag horizontal atau vertikal, pembacaan diagonal, ataupun pola baris dan kolom tertentu tergantung pada kunci yang digunakan. Variasi rute pembacaan inilah yang menjadi kekuatan utama dari *Route Cipher*, karena setiap pola pembacaan dapat menghasilkan kombinasi karakter yang sangat berbeda, bahkan jika *plaintext* dan kunci yang digunakan sama. Melalui penerapan *Route Cipher* sebagai lapisan kedua, pola pengacakan karakter yang telah terbentuk sebelumnya menjadi semakin kompleks. Hal ini membuat hubungan antara *plaintext* dan *ciphertext* semakin sulit dipetakan, sehingga upaya kriptanalisis untuk menebak struktur pesan asli menjadi lebih rumit.

3. RESULT

Proses enkripsi dilakukan dengan menggunakan algoritma *Rail Fence Cipher* dan *Route Cipher* secara berurutan. Pada tahap pertama, plaintext **SEMANGATBELAJAR** dienkripsi menggunakan *Rail Fence Cipher* dengan kunci 5. Proses penulisan huruf dilakukan menggunakan pola zig-zag sesuai jumlah rel, dan hasil penyusunan karakter dapat dilihat pada **Table 1.**

Table 1 Tabel proses enkripsi *rail fense cipher*

S								B						
	E						T		E					
		M				A				L				R
			A		G						A		A	
				N								J		

Table 1 menunjukkan pola penempatan karakter *plaintext* pada susunan rel, yang kemudian dibaca baris demi baris untuk menghasilkan *ciphertext*. Setelah melalui proses enkripsi tersebut, dihasilkan *ciphertext* pertama yaitu : **SBETEMALRAGAANJ**.

Ciphertext tersebut kemudian dienkripsi kembali menggunakan metode *Route Cipher* dengan kunci 3. *Ciphertext* disusun ke dalam bentuk grid sesuai panjang kunci, dan apabila terdapat ruang kosong pada grid maka ditambahkan karakter *dummy* untuk melengkapinya. Proses transformasi *Route Cipher* dapat dilihat pada **Figure 2**.

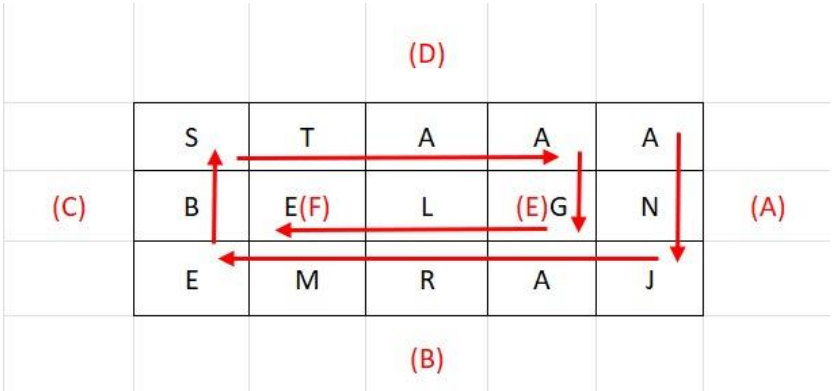

Figure 2 Proses enkripsi *route cipher*

Dari proses enkripsi ganda tersebut menghasilkan *ciphertext* kedua yaitu : **ANJARMEBSTAAGLE**.

Dengan penulisan *ciphertext* dimulai dari kiri ke kanan pada setiap baris, sedangkan proses penyandian *Route Cipher* menggunakan kunci searah jarum jam [6], kemudian *ciphertext* dibaca dari sisi kanan atas matriks dan berputar searah jarum jam/secara spiral dan dimulai dari baris kanan (A), baris bawah (B), baris kiri (C), baris atas (D) dan baris tengah (E) dan (F). Dapat dilihat pada **Figure 2** proses enkripsi *route cipher.*

Selain itu, dilakukan implementasi program menggunakan aplikasi web *Jupyter* dengan bahasa pemrograman menggunakan *python* untuk menguji proses enkripsi *Rail Fence Cipher* dan *Route Cipher*. *Source code* masing-masing metode ditampilkan pada **Figure 3**, **Figure 4**, dan **Figure 5**. Hasil eksekusi program menunjukkan bahwa proses enkripsi ganda berhasil menghasilkan *ciphertext* akhir sebagaimana diperlihatkan pada **Figure 6**.

Rail Fence & Route Cipher.py - C:\Users\advan\Downloads\Rail Fence & Route Cipher.py (3.13.0)

File Edit Format Run Options Window Help

```
# Rail Fence Cipher
def rail_fence_encrypt(plaintext, key):
    rail = [['\n' for _ in range(len(plaintext))] for _ in range(key)]
    dir_down = False
    row, col = 0, 0
    for char in plaintext:
        rail[row][col] = char
        col += 1
        if row == 0 or row == key - 1:
            dir_down = not dir_down
        row += 1 if dir_down else -1
    result = []
    for i in range(key):
        for j in range(len(plaintext)):
            if rail[i][j] != '\n':
                result.append(rail[i][j])
    return ''.join(result)

def rail_fence_decrypt(ciphertext, key):
    rail = [['\n' for _ in range(len(ciphertext))] for _ in range(key)]
    dir_down = None
    row, col = 0, 0
    for _ in range(len(ciphertext)):
        rail[row][col] = '*'
        col += 1
        if row == 0:
            dir_down = True
        elif row == key - 1:
            dir_down = False
        row += 1 if dir_down else -1
    index = 0
    for i in range(key):
        for j in range(len(ciphertext)):
            if rail[i][j] == '*' and index < len(ciphertext):
                rail[i][j] = ciphertext[index]
                index += 1
    result = []
    row, col = 0, 0
    for _ in range(len(ciphertext)):
        result.append(rail[row][col])
        col += 1
```

Figure 3 *Source code* enkripsi *Rail Fense Cipher*

Rail Fence & Route Cipher.py - C:\Users\advan\Downloads\Rail Fence & Route Cipher.py (3.13.0)

File Edit Format Run Options Window Help

```
        result.append(rail[row][col])
        col += 1
        if row == 0:
            dir_down = True
        elif row == key - 1:
            dir_down = False
        row += 1 if dir_down else -1
    return ''.join(result)

# Route Cipher
def route_traversal(matrix, order):
    result = [''] * len(order)
    index = 0
    for pos in order:
        row = (pos - 1) // len(matrix[0])
        col = (pos - 1) % len(matrix[0])
        result[index] = matrix[row][col]
        index += 1
    return ''.join(result)

def route_encrypt(plaintext, rows, order):
    cols = (len(plaintext) + rows - 1) // rows
    matrix = [['' for _ in range(cols)] for _ in range(rows)]

    index = 0
    for col in range(cols):
        for row in range(rows):
            if index < len(plaintext):
                matrix[row][col] = plaintext[index]
                index += 1

    cipher_text = route_traversal(matrix, order)
    return cipher_text

def route_decrypt(ciphertext, rows, order):
    cols = (len(ciphertext) + rows - 1) // rows
    matrix = [['' for _ in range(cols)] for _ in range(rows)]
    index = 0
    cipher_list = list(ciphertext)
    for pos in order:
        row = (pos - 1) // len(matrix[0])
```

Figure 4 *Source code* enkripsi *Route Cipher*

Rail Fence & Route Cipher.py - C:\Users\advan\Downloads\Rail Fence & Route Cipher.py (3.13.0)

File Edit Format Run Options Window Help

```
    for pos in order:
        row = (pos - 1) // len(matrix[0])
        col = (pos - 1) % len(matrix[0])
        matrix[row][col] = cipher_list[index]
        index += 1

    decrypted_text = ''
    for col in range(cols):
        for row in range(rows):
            if matrix[row][col] != '':
                decrypted_text += matrix[row][col]
    return decrypted_text

# Menu utama
def main():
    print("Pilih Metode:")
    print("1. Rail Fence Cipher")
    print("2. Route Cipher")
    choice = input("Masukkan pilihan (1/2): ").strip()

    if choice == "1":  # Rail Fence Cipher
        print("Pilih Operasi:")
        print("1. Enkripsi")
        print("2. Dekripsi")
        operation = input("Masukkan pilihan (1/2): ").strip()

        if operation == "1":
            plaintext = input("Masukkan plaintext: ")
            key = int(input("Masukkan jumlah kunci (key): "))
            ciphertext = rail_fence_encrypt(plaintext, key)
            print("Hasil Ciphertext:", ciphertext)
        elif operation == "2":
            ciphertext = input("Masukkan ciphertext: ")
            key = int(input("Masukkan jumlah kunci (key): "))
            plaintext = rail_fence_decrypt(ciphertext, key)
            print("Hasil Plaintext:", plaintext)
        else:
            print("Pilihan tidak valid!")

    elif choice == "2":  # Route Cipher
        print("Pilih Operasi:")
```

```
    elif choice == "2":  # Route Cipher
        print("Pilih Operasi:")
        print("1. Enkripsi")
        print("2. Dekripsi")
        operation = input("Masukkan pilihan (1/2): ").strip()

        # Route cipher order (adjust accordingly)
        route_order = [5, 10, 15, 14, 13, 12, 11, 6, 1, 2, 3, 4, 9, 8, 7]
        key = 3  # Jumlah baris

        if operation == "1":
            plaintext = input("Masukkan plaintext yang akan dienkripsi: ").strip()
            cipher_text = route_encrypt(plaintext, key, route_order)
            print(f"Ciphertext: {cipher_text}")
        elif operation == "2":
            cipher_text = input("Masukkan ciphertext untuk dekripsi: ").strip()
            decrypted_text = route_decrypt(cipher_text, key, route_order)
            print(f"Decrypted text: {decrypted_text}")
        else:
            print("Pilihan tidak valid!")
    else:
        print("Pilihan tidak valid!")

# Menjalankan fungsi utama
if __name__ == "__main__":
    main()
```

Figure 5 *Source code* enkripsi ganda Rail *Fense Cipher* dan *Route Cipher*

Figure 6 Hasil enkripsi dari proses enkripsi ganda *Rail Fense Cipher* dan *Route Cipher*

Hasil akhir menunjukkan bahwa kombinasi *Rail Fence Cipher* dan *Route Cipher* mampu menghasilkan *ciphertext* yang lebih acak dan sulit diprediksi, sehingga berpotensi meningkatkan keamanan pesan digital yang tidak memiliki akses atau kunci untuk mengetahui pesan tersebut.

4. DISCUSSION

Hasil yang diperoleh dari proses enkripsi menunjukkan bahwa teknik transposisi yang digunakan pada *Rail Fence Cipher* mampu mengubah susunan karakter asli menjadi pola baru berdasarkan pergerakan zig-zag. *Rail Fence Cipher* di kenal sebagai salah satu algortima klasik berbasis transposisi yang menyusun *plaintext* dalam bentuk baris dan kolom untuk menghasilkan struktur teks yang berbeda dari pesan asli [20]. Pola Zig-zag ini menciptakan permutasi karakter sehingga pesan lebih sulit di baca tanpa mengetahui jumlah rel sebagai kunci.

Tahap berikutnya menggunakan *Route Cipher* untuk memberikan lapisan enkripsi tambahan. *Route Cipher* bekerja dengan menempatkan *ciphertext* pertama ke dalam grid dan membacanya kembali berdasarkan suatu rute tertentu, dalam penelitian ini menggunakan pola spiral searah jarum jam. *Route Cipher* dianggap sebagai perluasan dari teknik transposisi yang digunakan pada *Rail Fence Cipher* karena menggunakan prinsip penyusunan karakter ke dalam matriks dengan aturan pembacaan yang lebih fleksibel dan kompleks [6]. Selain itu, proses enkripsi dan dekripsi pada *Route Cipher* dapat dijelaskan melalui pendekatan matematis dengan memanfaatkan indeks karakter, sehingga menghasilkan transformasi yang lebih terstruktur dan sistematis [21].

Penggabungan kedua teknik ini memberikan efek peningkatan keamanan, karena setiap tahap enkripsi mengubah struktur pesan dengan cara berbeda. *Rail Fence Cipher* mengacak susunan berdasarkan pola zig-zag, sementara *Route Cipher* memodifikasi pesan berdasarkan pola rute pada matriks. Kombinasi keduanya menyebabkan *ciphertext* akhir mempunyai pola yang sangat berbeda dari pesan asli, sehingga mempersulit pihak yang tidak berwenang untuk melakukan proses dekripsi tanpa mengetahui kedua kunci dan urutan algoritma

Dengan demikian, hasil penelitian ini menunjukkan bahwa enkripsi ganda menggunakan *Rail Fence Cipher* dan *Route Cipher* mampu menghasilkan pola penyandian yang lebih kompleks dan sulit diprediksi. Pendekatan ini dapat diterapkan sebagai salah satu alternatif pengamanan pesan digital berbasis algoritma trensposisi klasik, khususnya dalam konteks kebutuhan sistem keamanan data yang sederhana namun tetap memberikan tingkat perlindungan yang lebih baik.

5. CONCLUSION

Keamanan pesan menjadi aspek penting di era digital, saat pesan yang dikirim melalui jaringan internet dapat menimbulkan tantangan tersendiri dalam menjaga kerahasiaan dan integritas informasi. Kriptografi adalah ilmu yang mempelajari tentang keamanan dalam berkomunikasi yang mampu melindungi pesan dari akses yang tidak berwenang dengan mengimplementasikan algoritma, baik algoritma substitusi maupun transposisi. Penelitian ini menggabungkan dua algoritma transposisi, yaitu *Rail Fence* dan *Route Cipher*, untuk menciptakan proses enkripsi ganda sebagai bentuk pengamanan pesan digital yang menghasilkan *ciphertext* lebih kompleks dibandingkan penggunaannya secara terpisah. *Rail Fence* berfungsi untuk mengacak urutan karakter dalam bentuk pola zig-zag, sedangkan *Route Cipher* menata ulang karakter berdasarkan jalur tertentu dalam matriks pesan, sehingga memperkuat kerahasiaan dan meningkatkan tingkat kebingungan (*confusion*) pada hasil enkripsi. Kombinasi kedua algoritma ini memiliki kelebihan berupa keamanan yang lebih kuat, proses implementasi yang sederhana, serta hasil enkripsi yang akurat dan mudah diuji secara manual. Akan tetapi, kelemahannya meliputi potensi kerentanan terhadap serangan modern jika kunci yang digunakan terlalu pendek atau pola rute mudah ditebak, serta kurang efisien dalam menangani data berukuran besar tanpa optimasi proses. Untuk mengatasi keterbatasan tersebut, penelitian selanjutnya dapat mengintegrasikan metode kriptografi modern seperti *AES (Advanced Encryption Standard)* atau *RSA (Rivest–Shamir–Adleman)* sebagai lapisan tambahan guna meningkatkan kompleksitas dan keamanan sistem. Selain itu, pengujian terhadap berbagai jenis data, panjang karakter, serta variasi kunci dapat memberikan pemahaman yang lebih mendalam mengenai efektivitas kombinasi *Rail Fence* dan *Route Cipher* dalam berbagai skenario komunikasi digital. Dengan demikian, pendekatan ini diharapkan mampu menjadi solusi praktis dan efisien dalam menjaga keamanan pesan digital di tengah ancaman siber yang semakin berkembang. Penelitian selanjutnya, sistem enkripsi ganda ini dapat dikembangkan lebih lanjut melalui optimalisasi manajemen kunci, eksplorasi pola rute yang berbeda, serta integrasi dengan algoritma kriptografi modern untuk meningkatkan kinerja dan keamanannya.

6. REFERENCE

[1] "Kata kunci : virtual, account, transposisi-rail-fence," vol. 09, 2024.

[2] N. D. Girsang, "Kombinasi Algoritma Kriptografi Transposisi Rail Fence Cipher dan Route Cipher," vol. 2, no. November, pp. 48–53, 2019.

[3] M. Fadlan, E. Dianti Bintari, and A. Tasya, "Pengamanan Basis Data Dengan Algoritma Transposisi Rail Fence," *SIMKOM*, vol. 8, no. 2, pp. 66–72, Jul. 2023, doi: 10.51717/simkom.v8i2.135.

[4] Y. Suhelna, "Perancangan Aplikasi Penyandian Pesan Teks dengan Menggunakan Algoritma Digraph Cipher," vol. 2, pp. 25–34, 2020.

[5] N. Syah and E. Ardhianto, "Meningkatkan Keamanan Data Menggunakan Super Enkripsi Kombinasi Rail Fence dan Vigenere Autokey Pendahuluan Metode Penelitian," vol. 23, no. September, pp. 293–300, 2024.

[6] S. Bahri, F. Jihan, and B. Rudianto, "Implementasi Algoritma Super Enkripsi Vigenere Cipher Dan Route Cipher Pada Penyandian Pesan Teks," *J. Mat. UNAND*, vol. 12, no. 2, pp. 168–175, 2023.

[7] V. M. Hidayah, D. I. Mulyana, and Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," vol. 05, no. 03, pp. 8563–8573, 2023.

[8] D. Mulyana Iskandar *et al.*, "Penerapan Kriptografi AES pada Fres-Caesas: Perlindungan Pesan Teks dan Fail Dokumen Application of AES Cryptography in Fres-Caesas: Protection of Text Messages and Document Fails," *J. Inf. Technol. Comput. Sci.*, vol. 7, no. 3, 2024.

[9] L. Purnama, D. Iskandar Mulyana, Y. Maulana, E. Okta, and P. Sulaiman, "Terbit online pada laman web jurnal: https://ejurnalunsam.id/index.php/jicom/ Implementasi Algoritma One Time Mengggunakan Algoritma Chiper Transposition Sebagai Pengamanan Rahasia Pesan", [Online]. Available: https://ejurnalunsam.id/index.php/jicom/

[10] U. Hasanah, M. Fadli, F. Sahlan, and A. Sas, "Analisis Implementasi Pemerintahan Berbasis Elektronik (E – Government) Di Lingkungan Pemerintah Daerah Kabupaten Maros," vol. 2, no. 1, pp. 44–51, 2024, doi: 10.20895/jasmed.v2i1.1344.

[11] F. Fernando and M. A. I. Pakereng, "Implementasi Super Enkripsi Menggunakan Metode Rail Fence Cipher dan Metode Caesar Cipher Pada Data Pasien Klinik Eka Karigas," 2022.

[12] H. S. Disemadi, L. Sudirman, J. Girsang, and M. Aninda, "Perlindungan Data Pribadi di Era Digital : Mengapa Kita Perlu Peduli ?," *Sang Sewagati J.*, vol. 1, no. 2, pp. 67–90, 2023, [Online]. Available: https://journal.uib.ac.id/index.php/sasenal/article/view/8579

[13] S. J. Dinata, "Implementasi Algoritma Penyandian Transposisi Rail Fence pada Data Rekam Medis," *J. Inf.*

dan Teknol. Ilm., vol. 7, no. 3, pp. 305–309, 2020, [Online]. Available: https://www.ejurnal.stmik-budidarma.ac.id/index.php/inti/article/view/2406
[14] C. A. Sari and W. S. Sari, "Kombinasi Least Significant Bit (LSB-1) Dan Rivest Shamir Adleman (RSA) Dalam Kriptografi Citra Warna," vol. 13, no. 1, pp. 45–58, 2022.
[15] R. D. Zailani and A. Al Akbar, "Android-Based Cryptography Applications Using The Rail Fence Cipher Algorithm Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Rail Fence Cipher," vol. 2, no. 2, pp. 303–318, 2023.
[16] F. Siagian, "Super Enkripsi Algoritma Route Cipher Dan Algoritma Variably Modified Permutation Composition (Vmpc) Untuk Pengaman File Citra," *J. Teknol. Inf. Dan Komun.*, vol. 15, no. 1, pp. 146–154, 2024, doi: 10.51903/jtikp.v15i1.840.
[17] Z. Aufia and E. Alisah, "Enkripsi dan Dekripsi Pesan Menggunakan Metode Vigenere Cipher dan Route Cipher," vol. 1, no. 2, pp. 93–104, 2021.
[18] E. Noviyantono and M. Fadlan, "Studi Perbandingan Avalanche Effect pada Algoritma Kriptografi Transposisi untuk Meningkatkan Keamanan Data," vol. 9, pp. 1–5, 2024.
[19] D. Purnamasari and H. Prasetyani, "Analisis Performansi Kriptografi Berbasis Algoritma Caesar Cipher dan Rail Fence Cipher pada Tembang Macapat."
[20] R. S. Siregar, M. S. Asih, and N. Wulan, "Penerapan Algoritma RC4 dan Rail Fence untuk Enkripsi Database Mahasiswa pada Kampus POLTEKKES Kemenkes Medan," vol. 7, no. 2, pp. 51–56, 2019.
[21] A. P. Ramadhani, N. P. Tami, A. Lestari, and M. Erkamim, "Layered security model through integration of Vigenere and Hill Cipher in digital message encryption," vol. 2, no. 2, pp. 130–142, 2024, doi: 10.26905/jisad.v2i2.14005.
[22] A. P. Ramadhani, N. P. Tami, A. Lestari, and V. Wati, "Keamanan Data dengan Super Enkripsi Kombinasi Vigenere dan Atbash Cipher," vol. 04, no. 02, pp. 2–11, 2024

7. AUTHORS

Asih Lestari adalah mahasiswa jurusan Sistem Informasi Kota Cerdas Fakultas Teknik Universitas Tunas Pembangunan Surakarta. Email: f0223004_asihlestari@student.utp.ac.id

Nanda Putri Tami adalah mahasiswa jurusan Sistem Informasi Kota Cerdas Fakultas Teknik Universitas Tunas Pembangunan Surakarta. Email: f0223007_nandaputritami@student.utp.ac.id

Fabianus Delan Saputra adalah mahasiswa jurusan Sistem Informasi Kota Cerdas Fakultas Teknik Universitas Tunas Pembangunan Surakarta. Email: f0223002_fabianusdelansaputra@student.utp.ac.id

Erni Widarti adalah dosen di Program Studi Sistem Informasi Kota Cerdas, Fakultas Teknik, Universitas Tunas Pembangunan Surakarta. Minat riset penulis mencakup Gamification, Artificial Intelligence, Internet of Things, Machine Learning, dan Digital Transformation. Email: erni.widarti@lecture.utp.ac.id