JURNAL INSY PRO Information System and Processing
Volume 9, Nomor 1, Mei 2024 P–ISSN 2597-419X, E-ISSN 2579-468X
Ojs : http://journal.uinalauddin.ac.id/index.php/insypro
Email : insypro@uin-alauddin.ac.id

Studi Perbandingan Avalanche Effect pada Algoritma Kriptografi Transposisi untuk Meningkatkan Keamanan Data

Endyk Noviyantono[1)], Muhammad Fadlan[2)], Muhammad[3)], Suprianto[4)]

[1]Program Studi Teknik Informatika, STMIK PPKIA Tarakanita Rahmawati
[2,3]Program Studi Sistem Informasi, STMIK PPKIA Tarakanita Rahmawati
[4]Program Studi Manajemen Informatika, STMIK PPKIA Tarakanita Rahmawati
[1,2,3,4]Jl. Yos Sudarso No. 8, Tarakan, Kalimantan Utara, Indonesia

E-mail: endyk@ppkia.ac.id, fadlan@ppkia.ac.id[1)], muhammad@ppkia.ac.id[2)], supri@ppkia.ac.id[3)]

Abstrak – Beragam teknik kriptografi telah digunakan sebagai salah satu solusi dalam menjaga keamanan data, salah satunya ialah teknik transposisi yang termasuk dalam jenis kriptografi klasik. Penelitian ini bertujuan untuk melakukan studi komparatif terhadap dua teknik transposisi klasik, yaitu Transposisi Route dan Transposisi Rail Fence. Selain itu, penelitian ini bertujuan untuk mengetahui apakah beragam teknik transposisi klasik tersebut masih relevan dalam proses mengamankan data di era siber saat ini. Dalam penelitian ini, analisis komparasi dilakukan berdasarkan nilai Avalanche Effect (AE). Hasil penelitian menunjukkan bahwa teknik transposisi route memiliki nilai tertinggi dibandingkan teknik transposisi rail fence. Tetapi, berdasarkan standar minimal nilai AE menunjukkan bahwa kedua teknik tersebut masih berada pada posisi dibawah standar nilai minimal AE yaitu dibawah 50%.

Kata Kunci: Avalanche Effect, Komparasi, Kriptografi, Transposisi Rail Fence, Transposisi Route

Abstract *– Various cryptographic techniques have been used as a solution to maintain data security, one of which is the transposition technique which is included in the classic type of cryptography. This research aims to conduct a comparative study of two classic transposition techniques, namely Route Transposition and Rail Fence Transposition. Apart from that, this research aims to find out whether various classical transposition techniques are still relevant in the process of securing data in the current cyber era. In this research, comparative analysis was carried out based on the Avalanche Effect (AE) value. The research results show that the route transposition technique has the highest value compared to the rail fence transposition technique. However, based on the minimum standard AE value, it shows that the two techniques are still in a position below the minimum AE value, namely below 50%.*

Keywords: *Avalanche Effect, Comparison, Cryptography, Rail Fence Transposition, Route Transposition*

PENDAHULUAN

Dalam dunia yang semakin terhubung secara digital, keamanan data menjadi salah satu perhatian utama. Kriptografi adalah salah satu metode yang digunakan untuk menjaga kerahasiaan data dengan mengubah teks biasa menjadi teks terenkripsi yang sulit dipahami tanpa kunci yang sesuai (Abood & Guirguis, 2018; Qadir & Varol, 2019). Penggunaan ilmu kriptografi dengan berbagai jenis tekniknya selama ini telah dianggap mampu menjaga kerahasiaan data.

Seiring dengan berkembangnya teknologi informasi dalam membantu berbagai pekerjaan manusia harus diikuti dengan berbagai cara dalam menjaga keamanan data maupun informasi dari berbagai ancaman *(threat)* maupun kerentanan *(vulnerability)* terhadap penggunaan teknologi informasi (Saputro dkk., 2020; Yusfrizal, 2019). Salah satu teknik dasar yang banyak digunakan dalam menjaga keamanan data tersebut adalah melalui kriptografi teknik transposisi. Permasalahannya adalah teknik transposisi ini termasuk dalam teknik kriptografi klasik yang perlu dilakukan pengkajian ulang terkait dengan relevansi penggunaannya seiring dengan perkembangan teknologi yang semakin pesat. Terdapat beragam jenis teknik tranposisi dalam kriptografi, diantaranya Transposisi Route dan Transposisi Rail Fence.

Transposisi Rail Fence merupakan adalah metode kriptografi yang melibatkan pengurutan karakter dalam bentuk pola gelombang zigzag (turun-naik) (Girsang dkk., 2019; Nahar & Chakraborty, 2020), sedangkan Transposisi Route adalah salah satu teknik kriptografi yang mengenkripsi pesan dengan mengubah urutan karakter atau blok-blok tertentu sesuai dengan suatu kunci, yang kemudian diterapkan pada rute atau urutan tertentu untuk menghasilkan teks sandi yang sulit dibaca tanpa pengetahuan kunci yang tepat (Fitri

Wahyuni Lbn Tobing, 2019; Irdayani, 2019; Siska Bangun, 2019).

Beberapa penelitian terkait yang relevan dengan penelitian ini telah dilakukan, diantaranya penelitian yang bertujuan untuk melakukan perancangan sebuah aplikasi kriptografi dengan rail fence untuk menghasilkan pesan terenkripsi berbasis android. Proses enkripsi dan dekripsi dalam penelitian ini berhasil dilakukan dengan aplikasi yang telah dirancang (Febriani Purba & Puspasari, 2020).

Penelitian berikutnya menggunakan rail fence untuk mengamankan data rekam medis yang bersifat rahasia. Penelitian ini juga hanya berfokus pada perancangan sebuah aplikasi namun berbasis visual (Dinata, 2020). Hanya saja tidak ada melakukan pengukuran terkait dengan efektifitas algoritma yang digunakan.

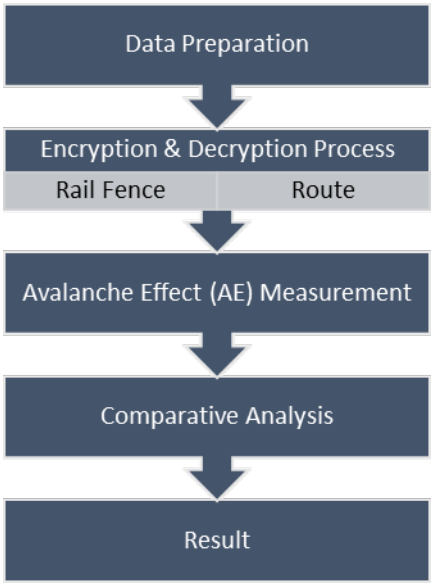
Penelitian untuk peningkatan keamanan teks juga telah dilakukan menggunakan perpaduan antara algoritma caesar dan rail fence. Proses enkripsi dalam penelitian ini dilakukan dalam dua tahapan sesuai dengan algoritma yang digunakan. Hasil penelitian menunjukkan bahwa aplikasi keamanan data yang dirancang berhasil melakukan proses enkripsi dan dekripsi sesuai dengan tahapan yang diusulkan (Jannah dkk., 2021).

Penelitian dengan menggunakan transposisi route juga telah dilakukan, antara lain peneltian yang menggunakan algoritma untuk untuk mengamankan file kerja berformat *.pdf* (Siska Bangun, 2019) hingga penggunaan algoritma transposisi route dalam proses keamanan file gambar atau citra (Irdayani, 2019). Dari beberapa penelitian tersebut memiliki kesamaan yakni penerapan algoritma transposisi route dan rail fence untuk mengamankan data. Namun, penelitian-penelitian tersebut belum melakukan proses pengujian lebih rinci terkait dengan tingkat keamanan dari algoritma yang diusulkan. Inilah landasan penelitian ini dilakukan untuk mengetahui tingkat keamanan dari algoritma transposisi route dan algoritma rail fence.

Penelitian ini bertujuan untuk melakukan studi perbandingan terhadap algoritma kriptografi klasik dengan teknik transposisi yang masih sering digunakan hingga saat ini. Selain itu, melalui penelitian ini juga akan diketahui apakah kedua teknik kriptografi klasik tersebut memiliki tingkat keamanan yang baik dan masih relevan jika digunakan di era siber saat ini. Dalam penelitian ini proses komparasi dilakukan melalui analisis terhadap nilai *Avalanche Effect* (AE). Avalanche effect adalah sifat dari sebuah algoritma kriptografi di mana perubahan kecil pada input atau pesan yang dimasukkan ke dalam algoritma tersebut menghasilkan perubahan besar dan acak dalam output yang terenkripsi. Pada penelitian ini, hasil nilai AE dari setiap algoritma akan dibandingkan antara satu dengan lainnya untuk mengetahui nilai AE terbaik.

METODOLOGI PENELITIAN

Jenis penelitian ini adalah penelitian komparatif. Penelitian dilakukan untuk membandingkan antara dua algoritma teknik transposisi dalam kriptografi, oleh karena itu dibutuhkan tahapan penelitian yang disusun dengan sistematis agar penelitian dapat dilakukan sesuai dengan tujuan awal penelitian ini. Adapun tahapan penelitian dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

Berdasarkan Gambar 1 tahapan penelitian yang pertama adalah *Data Preparation,* dalam tahapan ini beberapa data yang akan dijadikan sample penelitian akan disiapkan terlebih dahulu. Berikutnya, tahapan *Encryption Process* yang merupakan tahapan untuk melakukan proses enkripsi terhadap data atau teks asli yang telah disiapkan. Proses akan dilakukan baik menggunakan Transposisi Rail Fence maupun Transposisi Route.

Transposisi Rail Fence merupakan adalah metode kriptografi yang melibatkan pengurutan karakter dalam bentuk pola gelombang zigzag (turun-naik). Secara dasar, terdapat dua langkah dalam proses algoritma ini (Godara dkk., 2018):

a) Teks asli diatur secara diagonal dari atas ke bawah pada deretan yang berurutan sampai pada deretan terbawah, kemudian diatur kembali dari bawah ke atas dengan pola yang sama hingga deretan paling atas, pola ini diulang hingga setiap karakter teks asli ditulis pada deretan.
b) Setelah pengaturan karakter dilakukan seperti ini, karakter-karakter tersebut dibaca dari kiri ke kanan pada setiap deretan secara berurutan, dimulai dari deretan paling atas.

Secara sederhana dalam proses enkripsi transposisi route, 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. Proses dekripsi melibatkan penggunaan kunci yang sama untuk memulihkan pesan asli dengan mengembalikan urutan karakter atau blok-blok sesuai dengan rute yang telah ditentukan. Berikut tahapan dasar transposisi route yang dapat dibagi dalam tiga tahapan (Siska Bangun, 2019),

a) Pembuatan matriks dengan jumlah baris yang ditentukan berdasarkan pembagian jumlah plaintext dengan kunci.
b) Penentuan arah transposisi plaintext; misalnya, jika arah yang dipilih adalah spiral, ciphertext dihasilkan dengan membaca plaintext dalam matriks secara spiral
c) Selanjutnya, dalam proses dekripsi, algoritma route cipher hanya mengakses posisi berdasarkan urutan kata yang disusun dalam matriks, mengikuti susunan dari arah yang sama yang digunakan untuk membentuk ciphertext.

Tahapan berikutnya dalam penelitian ini adalah melakukan pengukuran nilai AE berdasarkan hasil dari tahapan yang kedua. Selanjutnya, hasil dari nilai AE tersebut akan dianalisis pada tahapan keempat sehingga dapat ditarik kesimpulan atau hasil terkait dengan algoritma mana yang lebih baik dari kedua algoritma tersebut dan apakah kedua algoritma tersebut memiliki tingkat keamanan yang cukup untuk digunakan diera siber saat ini. Adapun proses perhitungan nilai AE menggunakan Persamaan 1.

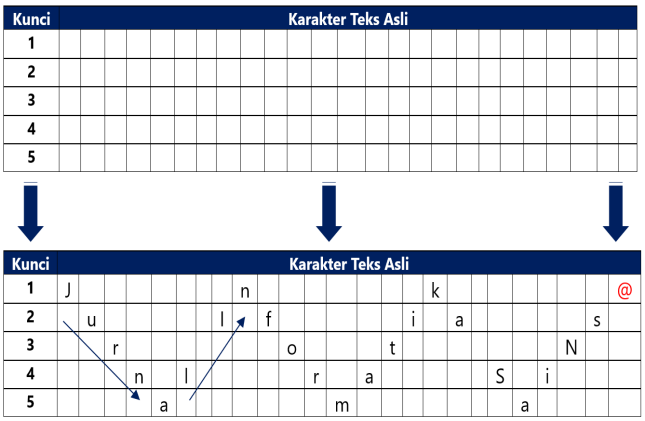
$$Nilai\ AE = Dx/total \times 100\% \quad (1)$$

Dimana, *Dx* mewakili jumlah bit yang berbeda, Nilai AE adalah hasil perhitungan dan total adalah jumlah total dari semua bit dalam data yang telah dienkripsi.

HASIL DAN PEMBAHASAN

a. Analisis Kinerja Transposisi Rail Fence

Proses transposisi rail fence dimulai dengan menyiapkan teks asli yang akan diacak menjadi teks sandi, misalnya teks asli yang akan digunakan sebagai sampel adalah Jurnal Informatika Sains, dengan kunci sebanyak 5 baris. Proses awal dilakukan dengan mengatur teks asli secara diagonal turun-naik dengan kedalaman sebanyak 5 baris (sesuai kunci). Adapun proses pengerjaan dapat dilihat pada Gambar 2.



Gambar 2. Proses Algoritma Rail Fence

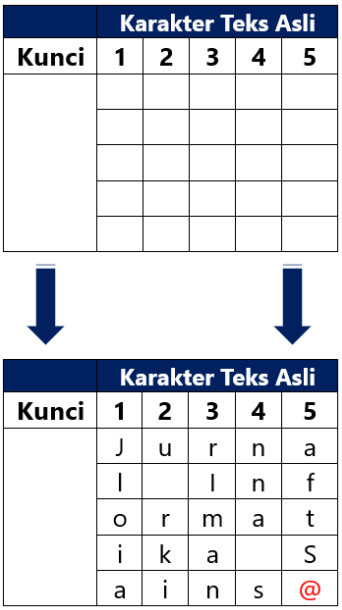
Dari Gambar 2 terlihat hasil dari proses pengaturan dari teks asli secara turun naik sesuai dengan pola dari rail fence. Dikarenakan pada baris kunci pertama di sel paling akhir tidak ada karakter yang mengisinya, maka sel kosong tersebut dapat di isi dengan karakter dummy, dalam hal ini ditentukan menggunakan karakter @. Berikutnya, teks sandi diambil dari kiri ke kanan dimulai dari baris kunci pertama (=1) sehingga didapatkan karakter teks sandi adalah *Jnk@ulfiasr ot NnIraSiama*.

Proses rail fence ini akan dilakukan terhadap beberapa sampel yang akan dijadikan perbandingan yang lebih lengkap dapat dilihat pada Tabel 1.

b. Analisis Kinerja Transposisi Route

Transposisi route diawali dengan membuat matriks sesuai dengan jumlah kunci yang telah ditentukan, setelah itu dipilih arah pembacaan terhadap teks sandi yang akan dihasilkan. Dalam contoh ini akan

digunakan sampel teks asli *Jurnal Informatika Sains*, dengan kunci sebanyak 5. Adapun proses pengerjaan dari algoritma ini dapat dilihat pada Gambar 3.



Gambar 3. Proses Algoritma Route

Dalam Gambar 3 terlihat bahwa yang pertama kali disiapkan adalah matriks sesuai dengan ukuran kunci yang telah ditetapkan. Berikutnya, mengisikan setiap karakter teks asli dalam matriks yang telah disiapkan. Pengisian dilakukan dimana tiap-tiap sel dari matriks akan diisikan oleh satu karakter teks asli yang disusun secara horizontal, dimana setelah karakter telah sampai pada kolom kunci terakhir (5) maka akan kembali mengisi sel pada baris berikutnya.

Proses pembacaan teks sandi dalam penelitian ini ditentukan dibaca dari pojok kanan bawah secara spiral menuju keatas, sehingga teks sandi yang terbentuk menjadi *@sniaika Stamroi InfanruJ.* Proses route ini akan dilakukan terhadap beberapa sampel yang akan dijadikan perbandingan yang lebih lengkap dapat dilihat pada Tabel 1.

c. Analisis Perbandingan berdasarkan Nilai AE

Proses komparatif dalam penelitian ini dilakukan berdasarkan nilai AE, pengujian dilakukan terhadap beberapa kasus uji. Kasus uji yang diberikan berupa plainteks yang akan diuji menggunakan transposisi rail fence dan transposisi route. Dalam penelitian ini, pengukuran nilai AE dilakukan dengan membandingkan dua hasil enkripsi terhadap plainteks yang sama, namun menggunakan kunci yang berbeda (diubah). Hal ini dikarenakan prinsip dasar dari pengukuran AE adalah bagaimana sedikit perubahan pada kunci dapat membawa perubahan yang signifikan terhadap hasil enkripsi.

Tidak semua kasus uji dapat digunakan dalam proses komparasi terhadap dua algoritma dalam penelitian ini, dikarenakan kasus uji melalui proses normalisasi terlebih dahulu dimana hanya kasus uji yang memiliki jumlah karakter yang sama antara hasil enkripsi menggunakan kunci awal dengan hasil enkripsi yang mengalami perubahan pada kunci, sehingga jika terdapat jumlah karakter yang berbeda maka kasus uji tersebut tidak akan digunakan dalam perhitungan AE. Setelah melalui proses normalisasi kasus uji, didapatkan beberapa kasus uji yang digunakan dalam proses komparasi. Adapun hasil komparasi tersebut dapat dilihat pada Tabel 1.

Tabel 1 Hasil Perbandingan

Data Uji	Total Karakter Asli	Rail Fence		Route	
		Bit Berbeda / Total Bit	Nilai AE	Bit Berbeda / Total Bit	Nilai AE
MF01	97	84 / 776	10,82	93 / 800	11,63
MF02	235	217 / 1880	11,54	218 / 1880	11,6
MF03	320	295 / 2560	11,52	299 / 2560	11,68
MF04	618	563 / 4944	11,39	572 / 4960	11,53
MF05	817	754 / 6536	11,54	753 / 6560	11,48
		Rerata	**11,36**	**Rerata**	**11,58**

Berdasarkan Tabel 1 terdapat lima kasus uji yang digunakan sebagai bahan komparasi dalam penelitian ini. Kelima kasus uji tersebut memiliki total karakter yang berbeda mulai karakter yang paling sedikit *(97 karakter)* hingga terbanyak *(817 karakter).* Pada Tabel 1 juga terdapat informasi mengenai jumlah bit yang berbeda dan total bit keseluruhan yang dihasilkan dari tiap-tiap proses enkripsi menggunakan algoritma rail fence dan algoritma route.

Hasil penelitian menunjukkan bahwa rata-rata nilai AE untuk algoritma rail fence sebesar *11,36%*, sedangkan algoritma route sebesar *11,58%.* Dapat disimpulkan bahwa nilai AE dari route cipher lebih tinggi dibandingkan rail fence. Namun, jika diperhatikan lebih lanjut kedua nilai AE tersebut tidak jauh berbeda. Ini dapat disebabkan kedua algoritma ini menggunakan prinsip yang sama yaitu teknik transposisi.

Disisi yang lain juga dapat disimpulkan bahwa kedua algoritma tersebut belum mampu mencapai standar minimal nilai AE yakni sebesar *50%.* Melalui penelitian ini dapat menunjukkan bahwa kedua algoritma tersebut memiliki tingkat keamanan yang

rendah jika digunakan untuk mengamankan data di era siber yang semakin pesat saat ini.

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dapat ditarik kesimpulan bahwa algoritma transposisi route dengan rata-rata nilai AE sebesar 11,58% memiliki nilai AE yang lebih tinggi dibandingkan dengan algoritma transposisi rail fence 11,36%. Namun, nilai rata-rata AE dari kedua algoritma transposisi tersebut belum mencapai nilai standar AE yaitu sebesar 50% jika ingin dikatakan sebagai algoritma yang memiliki tingkat keamanan yang baik. Disarankan untuk penelitian lebih lanjut jika ingin menerapkan algoritma transposisi klasik ini dapat dilakukan perpaduan antara dua metode dengan tujuan untuk menambah tingkat keamanan dari algoritma tersebut atau yang biasa juga dikenal dengan istilah teknik super enkripsi.

UCAPAN TERIMA KASIH

Terima kasih kepada pihak-pihak yang telah mendukung penelitian ini mulai dari awal pelaksanaan hingga publikasi.

DAFTAR PUSTAKA

Abood, O. G., & Guirguis, S. K. (2018). A Survey on Cryptography Algorithms. *International Journal of Scientific and Research Publications (IJSRP)*, *8*(7). https://doi.org/10.29322/ijsrp.8.7.2018.p7978

Dinata, S. J. (2020). *Implementasi Algoritma Penyandian Transposisi Rail Fence Pada Data Rekam Medis* (Vol. 7, Nomor 3).

Febriani Purba, D., & Puspasari, R. (2020). Penerapan Algoritma Rail Fence Untuk Penghasil Pesan Rahasia Berbasis Android Application of Rail Fence Algorithm for Producing Secret Messages Based on Android. *Jurnal FTIK*, *1*(1), 745–756.

Fitri Wahyuni Lbn Tobing, N. (2019). Perancangan Aplikasi Penyandian File Teks Menggunakan Algoritma Route Cipher Berbasis Dekstop. *Jurnal Pelita Informatika*, *8*(1).

Girsang, N. D., Siagian, H., Santoso, M. H., Wahyudi, A., & Sitorus, B. A. (2019). Kombinasi Algoritma Kriptografi Transposisi Rail Fence Cipher dan Route Cipher. *Prosiding Seminar Nasional Teknologi Informatika*, *2*, 48–53.

Godara, S., Kundu, S., & Kaler, R. (2018). An Improved Algorithmic Implementation of Rail Fence Cipher. *International Journal of Future Generation Communication and Networking*, *11*(2), 23–32. https://doi.org/10.14257/ijfgcn.2018.11.2.03

Irdayani. (2019). Keamanan Citra Menggunakan Algoritma Route Cipher. *Majalah Ilmiah INTI*, *6*(2), 246–249.

Jannah, M. H., Khairil, & Aspriyono, H. (2021). Implementasi Algoritma Caesar Chiper dan Rail Fence untuk Peningkatan Keamanan Teks Berbasis Client Server. *MEANS (Media Informasi Analisa dan Sistem)* , *6*(2), 184–187. https://doi.org/10.54367/means.v6i2.1527

Nahar, K., & Chakraborty, P. (2020). Improved Approach of Rail Fence for Enhancing Security. *International Journal of Innovative Technology and Exploring Engineering*, *9*(9), 583–585. https://doi.org/10.35940/ijitee.I7637.079920

Qadir, A. M., & Varol, N. (2019). A Review Paper on Cryptography. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. https://doi.org/10.1109/ISDFS.2019.8757514

Saputro, T. H., Hidayati, N., & Ujianto, E. I. H. (2020). Survei Tentang Algoritma Kriptografi Asimetris. *JIP (Jurnal Informatika Polinema)*, *6*(2). https://doi.org/10.33795/jip.v6i2.345

Siska Bangun, M. (2019). Implementasi Algoritma Route Cipher Dalam Pengamanan File Pdf. *Technology and Science (BITS)*, *1*(1).

Yusfrizal. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan RSA Berbasis Android. *Jurnal Teknik Informatika Kaputama (JTIK)*, *3*(2).