IMPLEMENTASI ALGORITMA TRANSPOSISI RAIL FENCE CIPHER UNTUK PENGAMANAN VIRTUAL ACCOUNT

Widyanti Masintan Siagian[1], Sinar Sinurat[2], Sony Bahagia Sinaga[3]
[1,2,3]Universitas Budi Darma, Medan
[1]widyantisiagian02@gmail.com, [2]sinurat.sin@gmail.com,
[3]sonybahagia@gmail.com

ABSTRAK

Pesatnya perkembangan teknologi informasi menjadikan informasi sebagai kebutuhan pokok bagi setiap orang. Seiring berkembangnya teknologi, maka keamanan terhadap kerahasiaan data dan informasi yang dipertukarkan akan semakin meningkat. Untuk mengelola virtual account terutama dari segi keamanan maka dibutuhkan suatu kata sandi. Kata sandi diperlukan saat melakukan transaksi, mengakses informasi akun atau melakukan perubahan pada pengaturan akun virtual. Tata cara keamanan kata sandi virtual account dapat bervariasi tergantung pada penyedia layanan atau lembaga keuangan yang mengelola virtual account. Penelitian ini bertujuan untuk menginvestigasi penggunaan salah satu algoritma dalam kriptografi, yaitu transposisi Rail Fence dalam mengamankan data pemasok. Penelitian ini menggunakan pendekatan eksperimental dengan menggunakan data pemasok untuk melakukan simulasi penerapan transposisi Rail Fence. Penelitian ini berkontribusi dalam penerapan enkripsi untuk melindungi basis data pemasok. Secara garis besar, hasil penelitian menunjukkan bahwa penggunaan metode Rail Fence dapat diterapkan untuk meningkatkan keamanan data pemasok dalam sebuah perusahaan.

Kata kunci : *virtual, account, transposisi-rail-fence*

ABSTRACT

The rapid advancement of information technology has made information a fundamental need for everyone. With the progression of technology, the security of data and information exchanged is increasingly important. To manage virtual accounts, especially regarding security, a password is essential. Passwords are required for transactions, accessing account information, or making changes to virtual account settings. The security procedures for virtual account passwords can vary depending on the service provider or financial institution managing the virtual account. This research aims to investigate the use of one cryptographic algorithm, Rail Fence transposition, in securing supplier data. The study employs an experimental approach using supplier data to simulate the application of Rail Fence transposition. This research contributes to the application of encryption to protect supplier databases. Overall, the results indicate that the Rail Fence method can be effectively implemented to enhance the security of supplier data within a company.

*Keywords**:** virtual, account, rail fence transposition*

A. Pendahuluan

Dengan kemajuan teknologi dan meningkatnya penggunaan transaksi digital, keamanan sandi virtual account menjadi isu yang sangat penting karena potensi risiko terkait dengan keamanan informasi keuangan (Ngamal, 2021). Saat ini, banyak pengguna yang cenderung memilih sandi yang lemah atau mudah ditebak, seperti nama atau tanggal lahir, yang membuat akun mereka rentan terhadap serangan (Komalasari, 2020);(Aksenta, 2023). Selain itu, kebijakan pengelolaan sandi yang kurang ketat pada beberapa platform atau layanan dapat meningkatkan risiko akses yang tidak sah. Oleh karena itu, pengamanan sandi virtual account sangat diperlukan untuk melindungi informasi keuangan pengguna, mencegah akses yang tidak sah, dan memitigasi risiko serangan siber.

Virtual account merupakan akun pembayaran digital yang digunakan untuk identifikasi pembayaran, berbeda dari nomor rekening fisik yang terkait langsung dengan bank atau lembaga keuangan (Muwaffaq & Akhmadi, 2022). Setiap virtual account memiliki nomor identifikasi unik yang digunakan untuk mengidentifikasi pemiliknya atau transaksi tertentu. Penelitian terdahulu oleh Tuti Nurhaeni menunjukkan bahwa virtual account dapat digunakan sebagai media pembayaran digital yang memudahkan transaksi bagi pengguna (Nurhaeni, 2016). Namun, untuk memastikan keamanan dari akun virtual ini, sangat penting untuk memiliki kata sandi yang kuat. Keamanan kata sandi pada virtual account menjadi aspek krusial dalam perlindungan informasi akun (Shofyan, 2024). Kata sandi diperlukan saat melakukan transaksi, mengakses informasi akun, atau melakukan perubahan pada pengaturan akun. Tata cara keamanan kata sandi dapat bervariasi tergantung pada penyedia layanan atau lembaga keuangan yang mengelola virtual account (Roberto, 2020). Penelitian oleh Dani Indra Junaedi menekankan bahwa kata sandi yang kuat harus mengandung kombinasi karakter angka, huruf (besar dan kecil), serta simbol (Junaedi, 2018). Semakin kompleks dan panjang karakter yang digunakan, semakin aman password tersebut, sehingga mengurangi risiko akses yang tidak sah.

Untuk meningkatkan keamanan virtual account, teknik kriptografi dapat diterapkan. Berbagai *algoritma kriptografi* dirancang untuk menyediakan tingkat keamanan tinggi dan melindungi data dari akses yang tidak sah. Salah satu algoritma yang digunakan dalam penelitian ini adalah algoritma *Transposisi Rail Fence Cipher*. Algoritma ini merupakan teknik enkripsi sederhana yang mengatur karakter dalam pola zig-zag dan membacanya per baris untuk menghasilkan teks terenkripsi, sehingga mengacak urutan karakter. Menurut penelitian oleh Fadlan, (2023) *algoritma Rail Fence Cipher* menggunakan pola segitiga atau rail fence untuk menyusun karakter-karakter dari teks terang (*plaintext*). Karakter-karakter ini diurutkan ke dalam baris-baris segitiga dan kemudian diambil berdasarkan pola tertentu. Dengan cara ini, pesan yang dikirimkan menjadi lebih sulit untuk dibaca oleh pihak yang tidak berwenang. Penelitian terdahulu oleh Dinata, (2020) juga menunjukkan bahwa algoritma Rail Fence Cipher merupakan bentuk cipher transposisi sederhana yang diinspirasi oleh model Polybius square. Polybius square menyusun huruf dalam matriks 5x5 dan mengkodekan huruf berdasarkan indeks cell matriks, mengganti posisi huruf tanpa menggunakan kunci khusus. Metode ini mengubah posisi karakter dalam teks sehingga teks terenkripsi menjadi tidak terbaca tanpa kunci yang benar.

Oleh karena itu, peneliti melakukan penelitian untuk menganalisis dan mengimplementasikan algoritma Transposisi Rail Fence Cipher dalam pengamanan sandi virtual account. Penelitian ini berjudul “Analisa dan Implementasi Algoritma Transposisi Rail Fence Cipher untuk Pengamanan Virtual Account” dan bertujuan untuk meningkatkan keamanan sandi virtual account dengan menggunakan teknik enkripsi yang efektif dan sederhana.

B. Metode Penelitian

Pada tahap pembuatan alur penelitian ini, sejumlah tahapan krusial harus dilakukan untuk memastikan penelitian berjalan dengan baik. Pertama, mengidentifikasi masalah adalah langkah awal yang melibatkan pemahaman dan analisis situasi untuk menentukan isu utama yang

perlu diperbaiki. Selanjutnya, kajian pustaka dilakukan untuk mengumpulkan materi dan referensi yang relevan dengan topik penelitian. Analisa sandi virtual account kemudian membahas bagaimana menganalisis sandi akun virtual. Tahapan berikutnya adalah dekripsi menggunakan algoritma Transposisi Rail Fence Cipher, di mana proses dekripsi dilakukan untuk mengembalikan sandi ke bentuk semula. Setelah itu, enkripsi menggunakan algoritma Transposisi Rail Fence Cipher dilakukan untuk mengamankan sandi virtual account. Kemudian, perancangan aplikasi dilakukan untuk merancang sistem keamanan virtual account berdasarkan hasil analisa dan metode yang telah dipilih. Pengujian bertujuan untuk menilai performa, keandalan, dan keamanan sistem yang dirancang, serta mengidentifikasi masalah atau kelemahan. Terakhir, dokumentasi penting untuk memelihara, berbagi, dan menyimpan informasi serta pengetahuan yang diperoleh selama proses penelitian

Sampel Data

Tujuan pengambilan sampel data adalah untuk mewakili karakteristik populasi secara umum tanpa harus mengumpulkan dan menganalisis semua data dari populasi tersebut. Sampel data ini digunakan dalam berbagai penelitian, survei, atau eksperimen sebagai cara untuk membuat estimasi atau kesimpulan tentang populasi yang lebih besar dengan biaya dan waktu yang lebih efisien.

Untuk sampel data yang digunakan sebagai objek penelitian ini adalah sandi akun *virtual account* penulis sendiri.

Plainteks 2 1 5 3 4 1 0 6 2

Untuk nilai desimal dari *plainteks* diambil dari nilai tabel ASCII 8 bit

C.Hasil Penelitian dan Pembahasan

Menentukan jenis virtual account yang akan diamankan adalah langkah awal dalam proses pengamanan. Pengamanan virtual account menggunakan kriptografi memerlukan kunci yang dapat dibagi menjadi beberapa bagian untuk keperluan enkripsi dan dekripsi. Algoritma transposisi Rail Fence Cipher digunakan untuk membagi dan mengelola kunci ini. Proses dimulai dengan mengenkripsi

plaintext virtual account menggunakan algoritma Rail Fence Cipher, yang menghasilkan ciphertext yang aman dan tidak dapat dibaca oleh pihak yang tidak berwenang. Untuk mengembalikan plaintext, dilakukan dekripsi menggunakan algoritma yang sama, memastikan bahwa hanya pihak yang berwenang yang dapat mengakses data tersebut. Setelah proses dekripsi selesai, pengguna dapat mengakses dan menggunakan data virtual account sesuai kebutuhan mereka.

Penerapan Algoritma *Transposisi Rail Fence Cipher*

Algoritma ini melibatkan penulisan *plainteks* sehingga mempunyai baris atas dan baris bawah yang terpisah. Urutan karakter pada baris atas akan diikuti oleh karakter berikutnya pada baris bawahnya, dan seterusnya sehingga n-rail. Apabila penulisan ke bawah sudah mencapai n, maka penulisan dilakukan ke baris atasnya dan seterusnya. Bila penulisan ke atas juga sudah mencapai n-rail, maka penulisan dilakukan seperti awal *ciphertext* dibaca secara horizontal. Pada penelitian untuk mengamankan *virtual account,* maka tuliskan teks asli dalam pola zig-zag pada sejumlah baris yang ditentukan (rel) selanjutkan baca karakter dari setiap baris secara berurutan untuk membentuk teks terenkripsi.

Proses Enkripsi

Proses enkripsi adalah untuk mengubah informasi atau data asli (plaintext) menjadi bentuk yang tidak dapat dibaca atau dimengerti (ciphertext) tanpa menggunakan kunci dekripsi yang tepat. Tujuan utama dari enkripsi adalah untuk melindungi kerahasiaan dan integritas data saat disimpan atau ditransmisikan, sehingga hanya pihak yang berwenang dapat mengakses informasi asli. Diasumsikan untuk teks *virtual account* yang akan di enkripsi adalah “215341062” (tidak termasuk tanda kutip), selanjutnya akan dilakukan proses pengamanan menggunakan algoritma *transposisi Rail Fence Cipher* dengan melakukan pergeseran 3. Maka hasil enkripsinya adalah :

2				4				2
	1		3		1		6	
		5				0		

Dalam proses Rail Fence, kedalaman atau jumlah baris ditentukan oleh pengirim pesan. Teks disusun secara zig-zag sesuai

kedalaman yang ditentukan, kemudian dibaca per baris. Setiap kata yang terbentuk dalam baris tersebut dibalik urutannya (reverse order) sebelum digabungkan menjadi satu dengan spasi sebagai pemisah antar baris. Sebagai contoh, jika baris pertama adalah "242", baris kedua "1316", dan baris ketiga "50", maka setelah proses reverse order, baris pertama tetap "242", baris kedua tetap "1316", dan baris ketiga berubah menjadi "05". Dengan demikian diperoleh cipherteksnya adalah 242131605

Proses Dekripsi

Proses dekripsi adalah nilai kunci yang digunakan adalah dengan menghitung jumlah karakter *ciphertext*, selanjutnya bagikan dengan nilai kunci enkripsi. Proses dekripsi dimulai dengan membalikkan urutan setiap baris Rail Fence, kemudian dilanjutkan dengan dekripsi. Langkah-langkah yang dilakukan adalah sebagai berikut:

2				3				5
	4		1		1		0	
		2				6		

Baris pertama dari teks yang diperoleh adalah 235, baris kedua adalah 4110, dan baris ketiga adalah 26. Setelah dilakukan reverse order pada setiap baris, hasilnya menjadi baris pertama 532, baris kedua 1041, dan baris ketiga 62.

2				4				2
	1		3		1		6	
		5				0		

Maka hasil dekripsi adalah “215341062”

Perancangan dan Pemodelan Sistem

Perancangan adalah gambaran dari pembuatan aplikasi pengamanan pesan teks akan membantu pengguna lebih mudah dalam menggunakan algoritma tersebut untuk mengamankan data atau pun informasi penting. Tujuan dari perancangan antarmuka yaitu membuat tampilan sistem yang sederhana dan mudah digunakan (*userfriendly*) sehingga *user* dapat lebih mudah dalam menggunakan sistem.

Implementasi

Implementasi merupakan langkah selanjutnya yang digunakan untuk mengoperasikan sistem yang dirancang. Sistem perancangan merupakan suatu kesatuan pengolahan yang terdiri dari prosedur dan pelaksanaan data. Penerapan sistem merupakan lanjutan dari tahap analisis dan pengujian sistem. Sistem

yang digunakan untuk implementasi dengan menggunakan bahasa pemrograman *visual basic 2008*.

Spesifikasi Sistem

Dalam menjalankan aplikasi, diperlukan fasilitas-fasilitas pendukung yang meliputi perangkat keras dan perangkat lunak. Untuk perangkat keras, disarankan menggunakan spesifikasi minimal berikut: prosesor minimal Core i3 2,3 GHz, memori minimal 1 GB, harddisk minimal 100 GB, VGA card minimal 1 GB, serta monitor dengan resolusi minimal 1024 × 768 piksel. Selain itu, keyboard dan mouse diperlukan jika menggunakan PC. Untuk perangkat lunak, diperlukan sistem operasi minimal Windows 7 dan aplikasi Visual Basic 2008 untuk implementasi aplikasi.

Tampilan Perangkat Lunak

Tampilan dari perangkat lunak pengamanan *Virtual Account* terlihat seperti gambar berikut ini.

1. Tampilan *Form* Utama

   Tampilan *form* menu utama terlihat seperti gambar berikut ini

Gambar 4.7 Tampilan Menu Utama

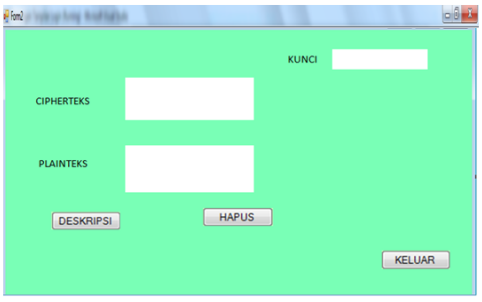
2. Tampilan *Form* Enkripsi

   Rancangan halaman menu enkripsi berfungsi untuk melakukan proses enkripsi. Tampilan halaman menu enkripsi dapat dilihat pada gambar berikut.

Gambar 4.8 Tampilan *Form* Enkripsi

3. Tampilan *Form* Dekripsi

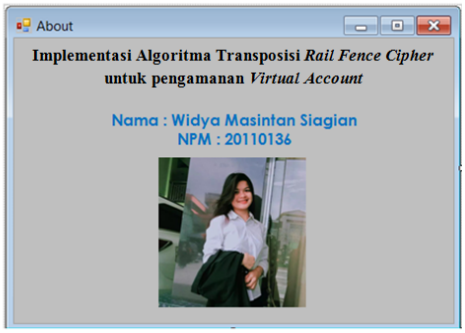
   Pada *form* ini akan ditampilkan proses deskripsi dengan menggunakan metode *Transposisi Rail Fence Cipher*. Adapun gambar proses tersebut dapat dilihat pada gambar.



Gambar 4.9 Tampilan *Form* Deskripsi

4. Tampilan *Form About*

   Form About merupakan *form* yang digunakan hanya menampilkan informasi tentang penulis.



Gambar 4.10 Tampilan *Form About*

E. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan mengenai pengamanan pesan teks, dapat disimpulkan bahwa penggunaan algoritma Transposisi Rail Fence Cipher untuk pengamanan virtual account menawarkan perlindungan yang signifikan terhadap data selama transmisi. Algoritma ini menyusun pesan dalam pola zig-zag dan membacanya per baris untuk menghasilkan teks terenkripsi, mengacak urutan karakter dan menyulitkan pihak yang tidak berwenang untuk mengakses informasi. Dengan demikian, sistem ini efektif dalam menjaga keamanan pesan teks sehingga hanya pihak yang berwenang yang dapat membacanya. Meskipun algoritma ini memberikan tingkat perlindungan yang baik, implementasi yang optimal sering kali memerlukan kombinasi metode enkripsi dan langkah-langkah keamanan tambahan, seperti penggunaan protokol komunikasi yang aman dan praktik pengelolaan kunci yang baik. Secara keseluruhan, algoritma *Rail Fence Cipher* merupakan alat yang bermanfaat dalam meningkatkan keamanan informasi digital, terutama dalam konteks *virtual account.*

DAFTAR PUSTAKA

Aksenta. (2023). LITERASI DIGITAL: Pengetahuan & Transformasi Terkini Teknologi Digital Era Industri 4.0 dan Sociaty 5.0. In *PT. Sonpedia Publishing Indonesia.*

Dinata, S. J. (2020). Implementasi Algoritma Penyandian Transposisi Rail Fence Pada Data Rekam Medis. *Jurnal Informasi Dan Teknologi Ilmiah (INTI)*, *7*(3), 305–309.

Fadlan, M. (2023). PENGAMANAN BASIS DATA DENGAN ALGORITMA TRANSPOSISI RAIL FENCE. *Jurnal Sistem Informasi Dan Sistem Komputer*, *8*(2), 66–72.

Junaedi, D. I. (2018). Peluang Keamanan Password dalam Transaksi Perbankan. *Jurnal Ilmu-Ilmu Informatika Dan Manajemen STMIK*, *12*(1), 25–33.

Komalasari, R. (2020). Kesadaran akan Keamanan Penggunaan Username dan Password. *TEMATIK - Jurnal Teknologi Informasi Dan Komunikas*, *3*(1).

Muwaffaq, F. A., & Akhmadi, M. H. (2022). PELAKSANAAN RESTRUKTURISASI DAN PENDEBITAN REKENING PENGELUARAN KAS NEGARA PADA KANTOR PELAYANAN PERBENDAHARAAN NEGARA KEDIRI. *Jurnal Info Artha*, *6*(1), 95–112.

Ngamal, Y. (2021). PENERAPAN MODEL MANAJEMEN RISIKO TEKNOLOGI DIGITAL BERKACA PADA CETAK BIRU TRANSFORMASI DIGITAL PERBANKAN INDONESIA. *Jurnal Manajemen Risiko*, *3*(1), 59–74.

Nurhaeni, T. (2016). RANCANGAN VIRTUAL ACCOUNT SEBAGAI MEDIA PEMBAYARAN. *ICIT*, *2*(2), 221–237.

Roberto. (2020). *Lebih Mengenal Digital Banking Manfaat, Peluang, dan Tantangan.*

Shofyan. (2024). Perancangan Dasbor yang Secure Scalable dan Reusable dengan Microservices Case Study. *Junal Teknologi*, *4*(1), 285–304.