ESCAF 2nd 2023
p-ISSN : 2962-7710

PENGAMANAN PESAN TEKS DENGAN TEKNIK TRANSPOSISI KARAKTER

Andysah Putera Utama Siahaan

Fakultas Sains dan Teknologi, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email: andiesiahan@gmail.com
Corresponding Author: Andysah Putera Utama Siahaan

ABSTRAK

Pesan merupakan informasi baik penting atau tidak yang dapat dibaca oleh penerima pesan. Pesan memiliki format teks yang digunakan dalam pengiriman data untuk memudahkan pengiriman dan mempercepat pengiriman data ke penerima pesan. Pesan teks merupakan format penyimpanan pesan dengan keamanan yang standard karena pesan memiliki panjang sesuai dengan karakter ASCII yang dapat secara langsung dibaca jika pesan tersebut ditemukan. Penelitian ini berkaitan dengan melakukan proses enkripsi dan dekripsi berdasarkan kunci yang digunakan untuk menentukan tata letak dari ciphertext. Kunci yang dibentuk merupakan blok persegi dengan ukuran 4 x 4. Hasil penelitian mendapatkan bahwa setiap plaintext dapat disusun menjadi ciphertext dengan baik berdasarkan pola kunci yang ditentukan pada kunci blok persegi

Kata Kunci: *enkripsi, dekripsi, persegi, keamanan*

I. PENDAHULUAN

Teknologi informasi pada saat ini telah memberikan inovasi dan kemajuan dalam hal pertukaran data. Pesan dapat dikirim melalui berbagai macam media yang dapat secara langsung diterima pada saat itu juga. Keamanan dalam pengiriman pesan sangat penting agar pesan tersebut terhindar dari tindak kejahatan digital yang dilakukan oleh pihak yang tidak bertanggung jawab. Pesan adalah bagian dari informasi lengkap yang memiliki arti dan tujuan bagi si penerima pesan tersebut. Pengiriman pesan pada umumnya dilakukan menggunakan media dengan bentuk pesan berjenis plaintext. Plaintext merupakan pesan yang berformat teks yang nilai panjang pesan tersebut sama dengan jumlah karakter yang ada pada pesan tersebut dimana pesan tersebut dapat langsung dibaca menggunakan text editor. Pengiriman pesan dengan format seperti ini bertujuan untuk memberikan kemudahan dan kecepatan pengiriman pada saat pesat tersebut dikirimkan. Pada umumnya, pesan dengan format teks memiliki kelemahan yang dapat secara langsung dibaca isinya tanpa memiliki pengamanan seperti kunci atau password pembuka. Hal ini akan menyebabkan kerugian bagi pengirim dan penerima pesan tersebut.

Pesan teks memiliki jumlah karakter yang minim yang terdiri dari huruf, angka dan beberapa karakter simbol tanda baca. Pesan ini memudahkan pengirim dan penerima pesan dalam melakukan komunikasi. Format pesan teks memiliki karakter yang terdiri dari karakter-karakter penting pada tabel ASCII seperti huruf besar, huruf kecil, dan angka. Pengiriman pesan teks perlu diamankan agar dapat memberikan kenyamanan bagi pengirim dan penerima pesan.

Penelitian ini membahas bagaimana memberikan keamanan pada pesan dengan teknik transposisi. Teknik ini akan menggunakan blok kunci dengan ukuran 4 x 4 dalam membangkitkan angka yang digunakan untuk melakukan pertukaran karakter antar plaintext. Hasil pertukaran akan dimasukkan ke blok ciphertext sehingga susunan pesan tersebut akan memiliki urutan atau indeks yang teracak. Ciphertext akan memiliki kandungan karakter yang identik

ESCAF 2nd 2023
p-ISSN : 2962-7710

dengan plaintext tetapi memiliki susunan atau posisi yang berbeda. Transposisi karakter diharapkan dapat memberikan keamanan pada plaintext sebelum pesan tersebut dikirimkan ke penerima pesan.

II. LANDASAN TEORI

Kriptografi

Kriptografi adalah ilmu yang berfungsi untuk memberikan keamanan pengiriman pesan antara pengirim dan penerima. Kriptografi merupakan tindakan mengacak teks biasa menjadi teks tersandi dan akan mengembalikan teks tersebut menjadi teks biasa kembali. Kriptografi juga mencakup penyamaran informasi dalam bentuk media lain agar tidak dapat terdeteksi oleh orang yang ingin mengambil pesan tersebut.

Enkripsi

Enkripsi adalah proses kriptografi yang berfungsi untuk melakukan transformasi karakter plaintext menjadi ciphertext. Proses ini dilakukan dengan menggunakan perhitungan matematika baik sederhana atau kompleks sehingga dapat menghasilkan pesan teracak.

Dekripsi

Dekripsi adalah kebalikan dari proses enkripsi yaitu proses transformasi karakter ciphertext menjadi plaintext. Proses ini mengembalikan pesan yang tidak dapat dibaca dengan baik menjadi pesan yang dapat dibaca oleh manusia sesuai dengan bahasa yang digunakan terhadap pesan tersebut sebelum dilakukan proses enkripsi. Pengembalian pesan tersebut juga harus menggunakan algoritma yang sama dengan pesan yang digunakan pada proses enkripsi.

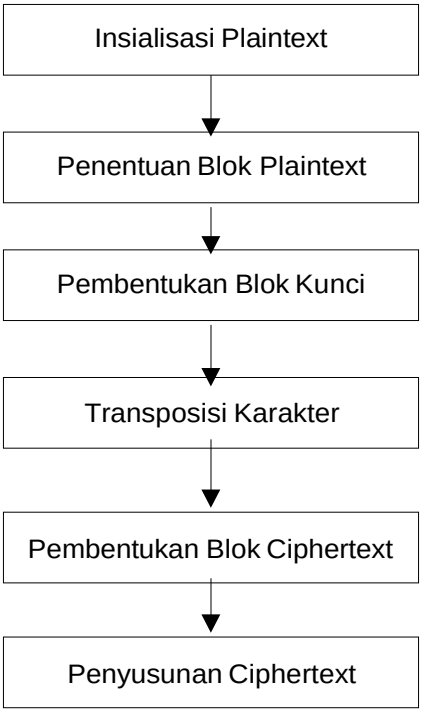
Transposisi Karakter

Dalam ilmu kriptografi, transposisi karakter yang disebut juga sebagai permutasi karakter adalah teknik pada proses enkripsi yang berfungsi untuk mengacak posisi karakter berdasarkan kumpulan karakter yang ada pada plaintext itu sendiri. Proses ini tidak mengubah karakter menjadi karakter lain atau yang disebut dengan substitusi. Transposisi karakter akan menyusun ulang karakter pada plaintext sesuai dengan algoritma atau formula bagaimana untuk mengacak urutan dari karakter tersebut. Transposisi karakter akan menghasilkan ciphertext yang merupakan hasil permutasi dari plaintext. Transposisi karakter berbeda jauh dengan substitusi karakter dimana proses substitusi karakter tidak mengubah posisi atau indeks dari plaintext, tetapi mengganti karakter plaintext dengan karakter lainnya sesuai dengan formula yang diberikan terhadap karakter tersebut.

III. METODOLOGI PENELITIAN

Tahapan Penelitian

Ada beberapa tahapan dalam melakukan penelitian pengamanan pesan dengan teknik transposisi karakter. Tahapan penelitian yang dilakukan penulis dapat dilihat pada gambar 1.



Gambar 1. Tahapan Penelitian

Gambar 1 menjelaskan tahapan penelitian yang dilakukan. Penjelasan terhadap gambar tersebut dapat dilihat sebagai berikut:

1. Inisialisasi Plaintext

Inisialisasi plaintext dilakukan dengan cara menentukan pesan teks yang akan digunakan.

2. Pembentukan Blok Plaintext
   Pembentukan blok plaintext dilakukan untuk membuat blok plaintext yang berukuran 4 x 4. Apabila plaintext tidak mencukupi ukuran blok, maka plaintext akan di padding dengan karakter lain agar dapat menempati blok dengan sempurna.
3. Pembentukan Blok Kunci
   Pembentukan blok kunci dilakukan untuk membangkitkan kunci yang berukuran 4 x 4 dengan angka yang tidak sama dengan urutan yang teracak.
4. Transposisi Karakter
   Transposisi karakter merupakan proses enkripsi yang digunakan pada penelitian. Transposisi akan memasukkan karakter plaintext dengan nomor urut yang terdaftar pada kunci ke blok ciphertext.
5. Pembentukan Blok Ciphertext
   Pembentukan blok ciphertext akan melakukan penyusunan hasil transposisi karakter menjadi pola blok persegi dengan ukuran 4 x 4.
6. Penyusunan Ciphertext
   Penyusunan ciphertext akan melakukan pemisahan karakter dari blok ciphertext sehingga menghasilkan deretan karakter ciphertext yang utuh.

Pembentukan Blok Kunci

Pembentukan blok kunci dilakukan dengan cara membentuk blok persegi dengan ukuran 4 x 4 yang digunakan sebagai penentu posisi karakter pada hasil enkripsi atau ciphertext. Proses pembentukan blok kunci dapat dilihat pada ilustrasi berikut ini.

Tabel 1. Indeks karakter pada plaintext

Y,X	1	2	3	4
1	0 (0,0)	1 (0,1)	2 (0,2)	3 (0,3)
2	4 (1,0)	5 (1,1)	6 (1,2)	7 (1,3)
3	8 (2,0)	9 (2,1)	10 (2,2)	11 (2,3)
4	12 (3,0)	13 (3,1)	14 (3,2)	15 (3,3)

Tabel 2. Indeks karakter pada ciphertext

Y,X	1	2	3	4
1	2 (0,2)	13 (3,1)	8 (2,0)	10 (2,2)
2	9 (2,1)	5 (1,1)	3 (0,3)	11 (2,3)
3	7 (1,3)	0 (0,0)	6 (1,2)	4 (1,0)
4	12 (3,0)	1 (0,1)	14 (3,2)	15 (3,3)

Tabel 1 adalah indeks atau daftar urutan pada plaintext. Dapat dilihat pada blok persegi tersusun angka 0 hingga 15 yang sebanyak 16 sel dengan urutan yang teratur. Tabel 2 adalah hasil pembentukan blok kunci yang sudah teracak susunan indeksnya,

IV. HASIL DAN PEMBAHASAN

Bagian hasil dan pembahasan akan menjelaskan hasil pengujian sistem atau program aplikasi yang dibangun untuk melaksanakan proses enkripsi dan dekripsi menggunakan transposisi karakter. Pengujian aplikasi terdiri dari 3 bagian, antara lain:

1. Pembentukan Blok Kunci
2. Enkripsi
3. Dekripsi

Plaintext Uji Coba

Plaintext uji coba pada penelitian menggunakan serangkaian karakter yang tersusun dalam bentuk satu paragraf yang berbunyi:

“Kriptografi adalah ilmu yang berfungsi untuk memberikan keamanan pengiriman pesan antara pengirim dan penerima. Kriptografi merupakan tindakan mengacak teks biasa menjadi teks

ESCAF 2nd 2023
p-ISSN : 2962-7710

tersandi dan akan mengembalikan teks tersebut menjadi plaintext."

Hasil Pembentukan Blok Kunci

Pembentukan kunci menggunakan teknik yang acak sehingga menghasilkan urutan indeks yang berbeda dari susunan indeks plaintext.

Gambar 1. Hasil pembentukan blok kunci

Gambar 1 menjelaskan hasil pembentukan kunci yang dibangkitkan oleh sistem. Pada bagian sebelah kiri dapat dilihat indeks plaintext yang sebelumnya masih tersusun dengan teratur dari mulai angka 0 hingga 15 secara horizontal. Pada bagian sebelah kanan, indeks tersebut sudah tersusun secara acak sehingga menghasilkan susunan yang berbeda. Tetapi pada saat proses pembentukan blok kunci ada beberapa indeks yang tidak mengalami perubahan seperti indeks ke 5, 12, 14, dan 15.

Hasil Proses Enkripsi

Proses enkripsi dilaksanakan dengan melakukan pembentukan blok plaintext terlebih dahulu dengan jumlah 16 karakter per blok. Berdasarkan plaintext yang digunakan hasil pembentukan blok plaintext dapat dilihat sebagai berikut.

Kriptografi adal [1]
ah ilmu yang ber [2]
fungsi untuk mem [3]
berikan keamanan [4]
pengiriman pesa [5]
n antara pengiri [6]
m dan penerima. [7]
Kriptografi meru [8]
pakan tindakan m [9]
engacak teks bia [10]
sa menjadi teks [11]
tersandi dan aka [12]
n mengembalikan [13]
teks tersebut me [14]
njadi plaintext. [15]

Pada hasil pembentukan blok tersebut, dapat dilihat karakter spasi juga terhitung sebagai karakter yang akan mengalami proses transposisi. Setelah dilakukan proses transposisi tersebut, blok ciphertext dapat dilihat sebagai berikut.

idaifop rKgtaral [1]
bynamig aul her [2]
nmnutigkuf s uem [3]
rnkaeaim bnkaean [4]
eemnain i rgppsa [5]
ai epannanrtg ri [6]
danre aiempnm . [7]
ieaifop rKgtmrru [8]
knnad akiptnaa m [9]
gbtkeaas ekc nia [10]
kd inmtasjeeas [11]
ra adnsnitda eka [12]
mablageimnenk n [13]
k sbetsurte teme [14]
axani dtlnpiejt. [15]

Hasil *ciphertext* yang diperoleh sudah berhasil mengubah posisi karakter dari plaintext sebelumnya sehingga tidak dapat dibaca dengan baik. Hasil enkripsi dinyatakan berhasil dalam memberikan kesulitan kepada orang yang ingin mendapatkan pesan teks.

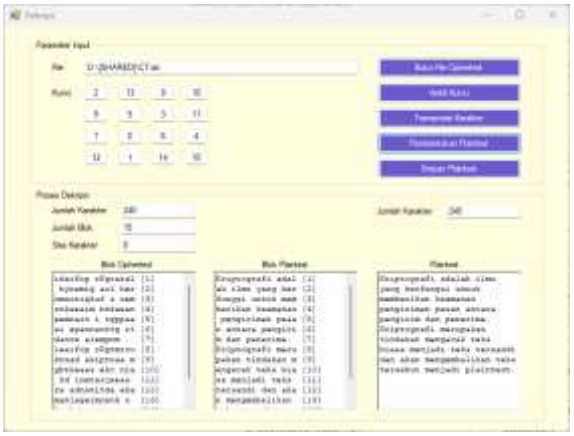
ESCAF 2nd 2023
p-ISSN : 2962-7710

Gambar 2. Hasil proses enkripsi

Gambar 2 menjelaskan hasil proses enkripsi yang dilakukan secara sistem. Hasil blok ciphertext memiliki hasil yang sama dengan penjelasan sebelumnya.

Hasil Proses Dekripsi

Proses dekripsi dilaksanakan dengan mengembalikan posisi karakter pada *ciphertext* sesuai dengan data kunci yang digunakan sebelumnya untuk melakukan transposisi karakter pada proses enkripsi.



Gambar 3. Hasil proses dekripsi

Gambar 3 menjelaskan proses dekripsi. Pada proses enkripsi sebelumnya, ciphertext telah disimpan dalam bentuk file teks. File tersebut akan diambil kembali untuk diproses lebih lanjut. File akan dibaca dan dimasukkan ke dalam blok ciphertext. Proses transposisi akan mengembalikan blok ciphertext ke blok plaintext. Setelah mendapatkan blok plaintext, proses selanjutnya akan merangkai blok tersebut menjadi plaintext utuh yang dapat dibaca oleh manusia.

Pembahasan

Setelah melakukan ujicoba terhadap proses pembentukan blok kunci, enkripsi dan dekripsi dilihat transposisi karakter yang dilakukan pada penelitian ini memiliki hasil yang baik. Kumpulan karakter yang dimiliki plaintext dapat dengan sempurna ditransposisikan menjadi ciphertext dan dikembalikan kembali menjadi plaintext. Jumlah karakter tersebut tidak mengalami pengurangan atau penambahan. Percobaan dilakukan dengan menggunakan 240 karakter yang terdiri dari 15 blok dimana setiap blok ditempati oleh 16 karakter. Ke 240 karakter tersebut berhasil dalam ujicoba enkripsi dan dekripsi.

V. KESIMPULAN

Transposisi karakter merupakan teknik yang dapat digunakan dalam mengubah indeks atau susunan plaintext sehingga dapat menghasilkan pesan yang tidak terbaca. Blok 4 x 4 akan menyusun posisi karakter dengan baik dan baik untuk memberikan kesulitan kepada orang yang akan mengambil pesan secara paksa. Kelemahan dari pembangkitan kunci adalah terkadang ada sebagian indeks yang tidak mengalami perubahan sehingga apabila terjadi pada karakter yang berdekatan, potongan ciphertext dapat terbaca tetapi tetap tidak dapat memberikan informasi seutuhnya kepada orang tersebut.

VI. DAFTAR PUSTAKA

M. Abror, “Pengertian dan Aspek-Aspek Keamanan Komputer,” 2018. [Online]. Available: https://www.ayoksinau.com/pengertian-dan-aspek-aspek-keamanan-komputer-lengkap/. [Accessed: 01-Oct-2018].

M. Iqbal, M. A. S. Pane, and A. P. U. Siahaan, “SMS Encryption Using One-Time Pad Cipher,” *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 54–58, 2016, doi: 10.9790/0661-18060205458.

S. Supiyandi, H. Hermansyah, and K. A. P. Sembiring, "Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video," *J. MEDIA Inform. BUDIDARMA*, vol. 4, no. 2, p. 340, Apr. 2020, doi: 10.30865/mib.v4i2.2042.

A. Cokro, "Belajar Kriptografi dan Steganografi," *Kumpulan Tutorial*, 2016. [Online]. Available: https://cokrowebberita.blogspot.com/2016/10/belajar-kriptografi-dan-steganografi.html. [Accessed: 01-Oct-2018].

A. P. U. Siahaan, "Rail Fence Cryptography in Securing Information," *Int. J. Sci. Eng. Res.*, vol. 7, no. 7, pp. 535–538, 2016.

A. A. Abdullah, R. Khalaf, and M. Riza, "A Realizable Quantum Three-Pass Protocol Authentication Based on Hill-Cipher Algorithm," *Math. Probl. Eng.*, vol. 2015, pp. 1–6, 2015, doi: 10.1155/2015/481824.

A. P. U. Siahaan, "Data Security Techniques Using Square Block Keys in Text Format," *Int. J. Res. Rev.*, vol. 10, no. 2, pp. 354–358, 2023, doi: 10.52403/ijrr.20230244.