

**MENJAGA KERAHASIAAN FILE DENGAN
MENGUNAKAN METODE RAIL FENCE
CIPHER DAN ROT13**

SKRIPSI

RANTOULI
0701163118



**PROGRAM STUDI ILMU KOMPUTER
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA
MEDAN
2022**

**MENJAGA KERAHASIAAN FILE DENGAN
MENGUNAKAN METODE RAIL FENCE
CIPHER DAN ROT13**

SKRIPSI

Diajukan untuk Memenuhi Syarat Mencapai Gelar Sarjana Komputer



**PROGRAM STUDI ILMU KOMPUTER
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA
MEDAN
2022**

PERSETUJUAN SKRIPSI

Hal : Surat Persetujuan Skripsi
Lamp : -

Kepada Yth,
Dekan Fakultas Sains dan Teknologi
UIN Sumatera Utara Medan

Assalamu'alaikum Wr. Wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengatakan pemikiran, maka kami selaku pembimbing berpendapat bahwa skripsi saudara,

Nama : Rantouli
Nomor Induk Mahasiswa : 0701163118
Program Studi : Ilmu Komputer
Judul : Menjaga Kerahasiaan File dengan Menggunakan Metode Rail Fence Cipher dan ROT13

Dapat disetujui untuk segera *dimunaqasyahkan*, Atas perhatiannya kami ucapkan terima kasih.

Medan, 30 Agustus 2022

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

Komisi Pembimbing,

Dosen Pembimbing I,



Muhammad Ikhsan, S.T., M. Kom
NIP. 198304154011011008

Dosen Pembimbing II,



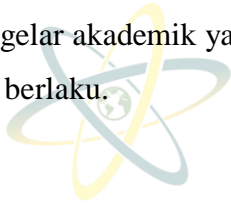
Abdul Halim Hasugian, M. Kom
NIB. 110000013

SURAT PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini :

Nama : Rantouli
Nomor Induk Mahasiswa : 0701163118
Program Studi : Ilmu Komputer
Judul : Menjaga Kerahasian File dengan Menggunakan Metode Rail Fence Cipher dan ROT13

Dengan ini menyatakan bahwa skripsi ini adalah hasil karya saya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya. Apabila dikemudian hari ditemukan plagiat dalam skripsi ini maka saya bersedia menerima sanksi pencabutan gelar akademik yang saya peroleh dan sanksi lainnya sesuai dengan peraturan yang berlaku.



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA

Medan, 30 Agustus 2022



Rantouli
0701163118

PENGESAHAN SKRIPSI

Nomor : B.305/ST/ST.V.2/PP.01.1/08/2023

Judul : Menjaga Kerahasiaan File dengan Menggunakan
Metode Rail Fence Cipher dan ROT13

Nama : Rantouli

Nomor Induk Mahasiswa : 0701163118

Program Studi : Ilmu Komputer


Fakultas : Sains dan Teknologi

Telah dipertahankan dihadapan Dewan Penguji Skripsi Program Studi Ilmu
Komputer Fakultas Sains dan Teknologi UIN Sumatera Utara Medan
dan dinyatakan **LULUS**.

Pada hari/tanggal : Selasa, 30 Agustus 2022

Media : Ruang Sidang Kampus UINSU

Tim Ujian Munaqasyah,
Ketua


Ilka Zufria, M. Kom
NIP. 198506042015031006

Penguji I,



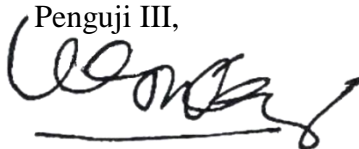
Muhammad Ikhsan, S.T., M. Kom
NIP. 198304152011011008

Penguji II,



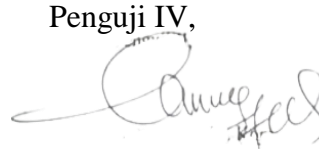
Abdul Halim Hasugian, M. Kom
NIB. 1100000113

Penguji III,



Heri Santoso, M. Kom
NIB. 1100000114

Penguji IV,



Armansyah, M. Kom
NIB. 1100000074

Mengesahkan,
Dekan Fakultas Sains dan Teknologi UIN Sumatera Utara
Medan,




Mhd Syahnan, M.A.
NIP. 196609051991031002

ABSTRAK

Transmisi informasi jarak jauh dengan menggunakan media internet dihadapkan pada masalah keamanan dan kerahasiaan data yang merupakan salah satu aspek penting dari komunikasi data, baik untuk tujuan keamanan data tersebut maupun untuk privasi individu. Salah satu media komunikasi adalah dengan menggunakan tulisan teks karena banyak informasi yang dapat disampaikan melalui tulisan (teks) dan terkadang dalam teks tersebut terdapat informasi yang bersifat rahasia. Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikannya. Algoritma *Rail Fence Cipher* memiliki keunggulan dibanding algoritma lainnya karena dalam tahap proses penulisan *plaintext* menjadi *ciphertext* dapat dilakukan pada baris mana saja sehingga menambah kerumitan proses enkripsi dan dekripsi. Algoritma *Rotate13* merupakan pengembangan dari algoritma *Caesar cipher* dimana algoritma ini melakukan pergantian setiap karakter huruf dengan 13 karakter di depan dan satu dibelakangnya sesuai dengan alfabet dimana dilakukan pergeseran karakter ke 13 yaitu pada huruf A diganti dengan N. Agar data tersamarkan dan tidak dapat terbaca dengan sekilas maka pergeseran karakter pada tabel ASCII dengan menggeser mundur sebanyak 13 karakter. Pada penelitian ini dilakukan enkripsi dan dekripsi dengan mengkombinasikan algoritma *Rail Fence Cipher* dengan *ROT13*, dimana proses enkripsi dan dekripsi dilakukan 2 kali. Berdasarkan hasil percobaan diperoleh hubungan antara waktu proses enkripsi dengan ukuran *plainteks* menunjukkan bahwa ada pengaruh kecepatan waktu proses berdasarkan jumlah panjang *plainteks* pada masing-masing algoritma serta berdasarkan hubungan antara waktu proses enkripsi dan waktu proses dekripsi menunjukkan bahwa waktu yang digunakan tidak memiliki perbedaan yang signifikan.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

Kata Kunci : Kriptografi klasik, *Rail Fence Cipher*, *Rotate13*

ABSTRACT

Transmission of information over long distances using internet media is faced with the problem of data security and confidentiality which is one of the important aspects of data communication, both for the purpose of data security and for individual privacy. One of the communication media is to use written text because a lot of information can be conveyed through writing (text) and sometimes in the text there is confidential information. Those who want their data not to be known by unauthorized parties always try to find ways to secure the information to be communicated. The Rail Fence Cipher algorithm has an advantage over other algorithms because in the process of writing plaintext into ciphertext it can be done on any line so that it adds to the complexity of the encryption and decryption process. The Rotate13 algorithm is a development of the Caesar cipher algorithm where this algorithm changes each letter character with 13 characters in front and one behind it according to the alphabet where the 13th character shift is carried out, namely the letter A is replaced with N. So that the data is disguised and cannot be read at a glance then shift the character in the ASCII table by shifting back as much as 13 characters. In this study, encryption and decryption were carried out by combining the Rail Fence Cipher algorithm with ROT13, where the encryption and decryption process is done 2 times. Based on the experimental results, the relationship between the encryption process time and the plaintext size shows that there is an effect of processing time speed based on the number of plaintext lengths in each algorithm and based on the relationship between the encryption process time and the decryption process time, it shows that the time used does not have a significant difference.

Keywords : Classic Cryptography, Rail Fence Cipher, Rotate13

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

KATA PENGANTAR



Assalamu'alaikum Wr. Wb.

Alhamdulillahirobbil'alamin, Puji syukur penulis ucapkan kepada Allah SWT atas yang telah memberikan rahmat dan karunia-Nya. Tak lupa juga sholawat dan salam kepada Nabi kita Muhammad SAW. Syukur Alhamdulillah kita ucapkan kehadiran Allah SWT, dimana atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul, **“Menjaga Kerahasiaan File dengan Menggunakan Metode Rail Fence Cipher dan ROT13”** sesuai dengan yang direncanakan. Penulis menyadari dalam penyusunan skripsi ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. H. Syahrin Harahap, MA, selaku Rektor Universitas Islam Negeri Sumatera Utara.
2. Bapak Dr. Mhd. Syahnan, MA, selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.
3. Bapak Ilka Zufria, M. Kom selaku Ketua Jurusan Ilmu Komputer Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.
4. Bapak Muhammad Ikhsan, ST., M. Kom selaku dosen pembimbing skripsi I yang telah berkontribusi membantu penulis dalam memberikan ide, saran, kritik, dan bimbingannya kepada penulis selama penulis mengerjakan skripsi ini.
5. Bapak Abdul Halim Hasugian, M. Kom selaku dosen pembimbing skripsi II yang telah berkontribusi membantu penulis dalam memberikan ide, saran, kritik, dan bimbingannya kepada penulis selama penulis mengerjakan skripsi ini.

6. Bapak Rakhmat Kurniawan R, S.T., M. Kom selaku Sekretaris Jurusan Ilmu Komputer Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.
7. Seluruh Tenaga Pengajar dan Pegawai Program Studi S1 Ilmu Komputer Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.
8. Teristimewa kedua malaikat selama hidup di dunia, Ibu kami Nur Asnia Nasution dan Bapak kami Sonang Situmorang yang selalu tulus melangitkan doa, memberikan motivasi dan semangat serta dukungan baik moril maupun materil seumur hidup penulis, terkhusus ketika menyelesaikan skripsi ini.
9. Teman-teman kelas Ilmu Komputer 4 yang selalu memberikan dukungan serta arahan kepada penulis.
10. Dan semua pihak yang telah membantu penulis namun tidak dapat disebutkan satu persatu. Penulis telah berusaha dengan segala upaya yang penulis lakukan dalam penyelesaian proposal skripsi ini.

Penulis menyadari sepenuhnya bahwa dalam pembuatan proposal skripsi ini masih jauh dari kesempurnaan, untuk itu kritik dan saran yang bersifat membangun sangat penulis harapkan dari pembaca demi sempurnanya skripsi ini. Semoga isi proposal skripsi ini bermanfaat dalam memperkaya khasanah ilmu pengetahuan bagi pembaca. *Amiiin Ya Rabbal'alamin.*

Wassalamu'alaikum Wr. Wb.

Medan, 4 Oktober 2022

Hormat Saya,



Rantouli

NIM. 0701163118

DAFTAR ISI

| | Halaman |
|--|----------------|
| ABSTRAK | i |
| ABSTRACT | ii |
| KATA PENGANTAR..... | iii |
| DAFTAR ISI..... | v |
| DAFTAR GAMBAR..... | vii |
| DAFTAR TABEL..... | viii |
| BAB I PENDAHULUAN | 1 |
| 1.1. Latar Belakang Masalah..... | 1 |
| 1.2. Rumusan Masalah | 4 |
| 1.3. Batasan Masalah..... | 4 |
| 1.4. Tujuan Penelitian..... | 4 |
| 1.5. Manfaat Penelitian..... | 4 |
| BAB II TINJAUAN PUSTAKA..... | 5 |
| 2.1. Algoritma | 5 |
| 2.2. File Teks..... | 5 |
| 2.3. Kriptografi..... | 6 |
| 2.3.1. Jenis-Jenis Algoritma Kriptografi..... | 9 |
| 2.3.2. Sejarah Kriptografi..... | 11 |
| 2.3.3. Algoritma Kriptografi Caesar Cipher | 11 |
| 2.3.4. Algoritma Rail Fence Cipher (RFC)..... | 15 |
| 2.3.5. Algoritma Rotate13 (ROT13)..... | 18 |
| 2.4. Visual Basic NET 2010..... | 21 |
| 2.5. Flowchart..... | 25 |
| 2.6. Penelitian Terdahulu | 27 |
| BAB III METODE PENELITIAN | 34 |
| 3.1. Tempat dan Waktu Penelitian | 34 |
| 3.1.1. Tempat Penelitian | 34 |
| 3.1.2. Waktu dan Jadwal Pelaksanaan Penelitian | 34 |

| | |
|--|-----------|
| 3.2. Bahan dan Alat Penelitian | 35 |
| 3.2.1. Perangkat Keras | 35 |
| 3.3. Perangkat Lunak..... | 35 |
| 3.4. Metodologi Penelitian | 35 |
| 3.4.1. Teknik Pengumpulan Data..... | 37 |
| 3.4.2. Perancangan Sistem | 37 |
| 3.4.3. Penerapan dan Pengujian | 39 |
| 3.4.3.1. Penerapan | 39 |
| 3.4.3.2. Pengujian | 39 |
| BAB IV PEMBAHASAN DAN HASIL..... | 40 |
| 4.1. Pembahasan..... | 40 |
| 4.1.1. Analisis Data | 40 |
| 4.1.2. Analisis Kebutuhan | 40 |
| 4.1.3. Flowchart Enkripsi Algoritma Rail Fence Cipher | 41 |
| 4.1.4. Flowchart Algoritma Rail Fence Cipher dan ROT13 | 43 |
| 4.1.5. Flowchart Enkripsi Rail Fence Cipher dan ROT13 | 44 |
| 4.1.6. Proses Enkripsi Algoritma ROT13 | 45 |
| 4.1.7. Proses Dekripsi Algoritma Rail Fence Cipher | 46 |
| 4.1.8. Proses Dekripsi Rail Fence Cipher | 51 |
| 4.1.9. Perancangan Antarmuka | 52 |
| 4.1.10. Gambar Tampilan | 53 |
| 4.2. Hasil Pengujian | 55 |
| BAB V KESIMPULAN DAN SARAN | 58 |
| 5.1. Kesimpulan..... | 58 |
| 5.2. Saran..... | 58 |
| DAFTAR PUSTAKA | 60 |

DAFTAR GAMBAR

| Gambar | Judul Gambar | Halaman |
|---------------|---|----------------|
| 2.1. | Skema Enkripsi dan Deskripsi dengan Menggunakan Kunci | 9 |
| 2.2. | Skema Algoritma Simetris (Arifah & Basuki, 2017)..... | 10 |
| 2.3. | Skema Algoritma Asimetris (Arifah & Basuki, 2017)..... | 10 |
| 2.4. | Proses Pergantian Huruf Pada Caesar Cipher | 12 |
| 2.5. | Alur Pergeseran $k=13$ | 19 |
| 2.6. | Hasil Pergeseran $k=13$ | 19 |
| 2.7. | Halaman Start Page Visual Studio Ultimate | 24 |
| 2.8. | Jendela New Project (Budiharto & Lisangan, 2012)..... | 24 |
| 2.9. | IDE Microsoft Visual Basic NET 2010 | 25 |
| 3.1. | Flowchart Enkripsi dan Dekripsi..... | 25 |
| 4.1. | Flowchart Hybrid Rail Fence Cipher dan ROT13..... | 42 |
| 4.2. | Flowchart Deskripsi Rail Fence Cipher dan ROT13 | 43 |
| 4.4. | Rancangan Form Menu | 53 |
| 4.5. | Tampilan Form Menu..... | 54 |
| 4.8. | Tampilan Form Enkripsi | 54 |
| 4.9. | Tampilan Running Time Enkripsi..... | 57 |

DAFTAR TABEL

| Tabel | Judul Tabel | Halaman |
|--------------|---|----------------|
| 2.1. | Tabel Substitusi ROT13 | 13 |
| 2.2. | Susunan Alfabet ROT13 | 14 |
| 2.3. | Proses Enkripsi Rail Fence Cipher | 16 |
| 2.4. | Susunan Ciphertext Baris 9 | 16 |
| 2.5. | Hasil Deskripsi Rail Fence Cipher | 17 |
| 2.6. | Proses Enkripsi Rail Fence Cipher | 17 |
| 2.7. | Susunan Cipher Baris 4 | 18 |
| 2.8. | Enkripsi ROT13 | 20 |
| 2.9. | Substitusi Ciphertext ke ASCII | 20 |
| 2.10. | Substitusi ASCII ke Abjad | 21 |
| 2.11. | Enkripsi Abjad ke Hexadecimal | 21 |
| 2.12. | Substitusi ASCII Hexa ke Abjad | 22 |
| 2.13. | Enkripsi ROT13 | 22 |
| 2.14. | Deskripsi ROT13 | 22 |
| 2.15. | Simbol-Simbol Flowchart Program (Jogiyanto, 2005) | 26 |
| 2.16. | Penelitian Terdahulu | 27 |
| 3.1. | Waktu dan Jadwal Penelitian | 34 |
| 4.1. | Proses Enkripsi Rail Fence Cipher | 44 |
| 4.2. | Tabel Alfabet dan Indeks | 45 |
| 4.3. | Hasil Enkripsi ROT13 | 45 |
| 4.4. | Hasil Dekripsi ROT13 | 48 |
| 4.5. | Proses Dekripsi Rail Fence Cipher | 50 |
| 4.6. | Hasil Deskripsi Rail Fence Cipher | 51 |
| 4.7. | Hasil Pengujian Enkripsi | 51 |
| 4.8. | Waktu Proses Enkripsi | 57 |

DAFTAR LAMPIRAN

| Lampiran | Judul Lampiran |
|----------|----------------------|
| 1. | Listing Program |
| 2. | Kartu Bimbingan |
| 3. | Daftar Riwayat Hidup |



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN