IMPLEMENTASI ALGORITMA KRIPTOGRAFI *RAIL FENCE* UNTUK MENGAMANKAN TEKS UJIAN

Skripsi

diajukan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana

Pendidikan Program Studi Pendidikan Teknik Informatika dan Komputer

Oleh

Muhammad Sufyan Tsauri

NIM. 5302414037

PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS NEGERI SEMARANG

2019

PERSETUJUAN PEMBIMBING

Nama	: Muhammad Sufyan Tsauri
NIM	: 5302414037
Program Studi	: Pendidikan Teknik Informatika dan Komputer
Judul	: Implementasi Algoritma Kriptografi *Rail Fence* untuk Mengamankan Teks Ujian

Skripsi ini telah disetujui oleh pembimbing untuk diajukan sidang panitia ujian skripsi Program Studi Pendidikan Teknik Informatika dan Komputer, Fakultas Teknik Universitas Negeri Semarang.

Semarang, November 2018

Pembimbing

Arief Arfriandi, S.T., M.Eng.

NIP. 198208242014041001

HALAMAN PENGESAHAN

Skripsi dengan judul "Implementasi Algoritma Kriptografi Rail Fence untuk Mengamankan Teks Ujian" telah dipertahankan di depan sidang Panitia Ujian Skripsi Fakultas Teknik UNNES pada Januari tahun 2019.

Oleh

Nama : Muhammad Sufyan Tsauri

NIM : 5302414037

Program Studi : Pendidikan Teknik Informatika dan Komputer

Panitia :

Ketua Panitia	Sekretaris
Dr.-Ing. Dhidik Prastiyanto, S.T., M.T.,	Ir. Ulfah Mediaty Arief, M.T.
NIP. 197805312005011002	NIP. 196605051998022001

Penguji 1	Penguji 2	Penguji 3/Pembimbing
Dr. Djuniadi, M.T.	Drs. Isdiyarto, M.Pd.	Arief Arfriandi, S.T., M.Eng.
NIP. 196306281990021001	NIP. 195706051986011001	NIP. 198208242014041001

Mengetahui:

Dekan Fakultas Teknik

Dr. Nur Qudus, M.T.

NIP. 196911301994031001

PERNYATAAN KEASLIAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini, adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, magister, dan doktor) baik di Universitas Negeri Semarang (UNNES) maupun perguruan tinggi lain.
2. Karya tulis ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan Pembimbing dan masukan Tim Penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari ditemukan terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya ini, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi ini.

Semarang, Desember 2018

Yang membuat pernyataan,

Muhammad Sufyan Tsauri

NIM. 5302414037

MOTTO DAN PERSEMBAHAN

Motto

- “Allah tidak membebani seseorang itu melainkan sesuai dengan kesanggupannya” (QS. Al-Baqarah: 286).
- Good people don’t say hurtful things (Muhammad Sufyan Tsauri).

Persembahan

Skripsi ini penulis persembahkan kepada :

- Allah SWT yang tak henti-hentinya memberikan kemudahan dan kelancaran dalam penyusunan skripsi ini.
- Kedua orang tua saya, Ibu Alimatul Mursyidah dan Bapak Abdul Rahman, yang selalu memberikan doa, dukungan, serta semangat.
- Seluruh teman-teman PTIK UNNES angkatan 2014 yang telah dan tengah berjuang bersama-sama menyelesaikan studinya.

ABSTRAK

Tsauri, Muhammad Sufyan. 2018. “Implementasi Algoritma Kriptografi *Rail Fence* untuk Mengamankan Teks Ujian”. Pembimbing : Arief Arfriandi, S.T., M.Eng. Pendidikan Teknik Informatika dan Komputer.

Perkembangan teknologi yang semakin pesat membuat dokumen dalam kehidupan kita ikut berkembang menjadi data digital. Dengan perubahan tersebut muncul masalah baru mengenai keamanan data, terutama dalam hal kerahasiaan ketersediaan dan integritas data. Untuk mengatasi permasalahan tersebut, teknik kriptografi dapat digunakan untuk menanggulangi masalah keamanan dan privasi tersebut salah satunya yaitu algoritma *rail fence*. Dengan menggunakan algortima *rail fence* dan implementasi algoritma ke dalam sistem diharapkan dapat digunakan untuk mengamankan data teks digital.

Tahapan dalam penelitian ini yaitu dengan melakukan indentifikasi masalah, studi pustaka, analisa kebutuhan, pemodelan sistem, penulisan kode, pengujian algoritma, dan mengambil kesimpulan dari hasil penelitian. Teknik pengujian yang digunakan adalah uji *white-box* yaitu menganalisis kerja internal dan struktur sebuah perangkat lunak.

Berdasarkan pengujian *white-box basis path testing* terhadap algoritma enkripsi dan dekripsi diketahui bahwa tingkat kompleksitas program mendapat nilai kompleksitas 8 untuk proses enkripsi dan nilai kompleksitas 8 untuk proses dekripsi sehingga kode struktur program termasuk ke dalam kode yang terstruktur dan telah ditulis dengan baik.

Hasil implementasi dan pengujian algoritma *rail fence* menunjukkan bahwa sistem yang telah dibuat dapat digunakan untuk mengamankan data teks digital pada *database* dan memperoleh hasil uji yang valid. Diharapkan pada penelitian selajutnya algoritma *rail fence* dapat diimplementasikan bersama dengan algoritma lainnya untuk memperkuat tingkat keamanan enkripsi.

Kata Kunci: Kriptografi, *Rail Fence*, Sistem Keamanan, Teks

KATA PENGANTAR

Puji dan syukur penulis ucapkan ke hadirat Allah SWT yang telah melimpahkan rahmat serta karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Algoritma Kriptografi Rail Fence untuk Mengamankan Teks Ujian". Skripsi ini disusun sebagai salah satu persyaratan meraih gelar Sarjana Pendidikan pada Program Studi S1 Pendidikan Teknik Informatika dan Komputer Universitas Negeri Semarang. Penyelesaian skripsi ini tidak lepas dari bantuan berbagai pihak, oleh karena itu penulis menyampaikan ucapan terima kasih kepada :

1. Prof. Dr, Fathur Rokhman, M.Hum., Rektor Universitas Negeri Semarang atas kesempatan yang diberikan kepada penulis untuk menempuh studi di Universitas Negeri Semarang.
2. Dr. Nur Qudus, M.T., Dekan Fakultas Teknik, Dr. Ing. Dhidik Prastiyanto, S.T., M.T., Ketua jurusan Teknik Elektro, Ir. Ulfah Mediaty Arief, M.T., Ketua program studi Pendidikan Teknik Informatika dan Komputer atas fasilitas yang telah disediakan bagi mahasiswa.
3. Bapak Arief Arfriandi, S.T., M.Eng., selaku dosen pembimbing yang telah memberikan bimbingan, arahan, nasehat serta motivasi dalam penulisan karya ini
4. Seluruh dosen Jurusan Teknik Elektro Fakultas Teknik Universitas Negeri Semarang yang telah banyak memberi bekal pengetahuan yang berharga.

5. Teman-teman mahasiswa PTIK Universitas Negeri Semarang angkatan 2014 yang saling memberikan semangat, perhatian, dan penguatan.
6. Berbagai pihak yang telah memberi bantuan untuk penyusuan skripsi ini yang tidak dapat penulis sebutkan satu persatu.

Penulis hanya dapat memanjatkan doa semoga semua pihak yang telah membantu penuls dalam penyusunan skripsi ini mendapatkan pahala dari Allah SWT. Semoga skripsi ini dapat bermanfaat dan memberikan sumbangan yang berarti bagi pihak yang membutuhkan.

Semarang, Januari 2019

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi digital yang berkembang sangat pesat pada beberapa tahun terakhir dan menghasilkan berbagai hal yang dapat membantu meringankan pekerjaan manusia. Dengan perkembangan yang sedemikian pesat, dokumen dalam kehidupan kita pun ikut berkembang menjadi data digital. Dari berbagai macam bentuk data digital salah satunya adalah teks ujian yang digunakan untuk ujian online. Dengan beralihnya teks ujian menjadi data digital, rentannya keamanan data menjadi permasalahan baru yang harus diatasi, terutama mengenai kerahasiaan ketersediaan dan integritas data.

Dalam laporan tahunan mengenai kerugian pelanggaran/kebocoran data yang dipublikasikan oleh (Ponemon Institute LLC, 2018), menyebutkan bahwa pada tahun 2018 rata-rata kerugian yang diderita dari kebocoran data mencapai 3.86 juta dollar pertahun. Penyebab utama dari permasalahan tersebut terbagi menjadi 3 bagian, yaitu *criminal attack* (48%), *human error* (27%), dan *system glitch* (25%).

Permasalahan mengenai kebocoran data tentu bukan hal yang bisa diabaikan, misal saja pada sektor kesehatan dimana rumah sakit memiliki banyak data pribadi baik itu *personally indentiable information* (PII) maupun *protected health information* (PHI), ancaman terhadap data tersebut tentunya akan bertambah pada masa mendatang. Informasi medis pasien yang diretas oleh *cyber-crime* dapat diperjual belikan dengan nilai 10 kali lipat pada *black market*. Data pada *black*

market tersebut kemudian dapat digunakan untuk membayar pinjaman bank, pengembalian uang pajak, paypal, dan lain sebagainya (Floyd, et al., 2016).

Menurut (Hastaka, 2017), data soal ujian pada komputer dapat dibongkar dengan mudah oleh pihak dari luar jika hanya mengandalkan keamanan dasar yang terdapat dari komputer tersebut. Salah satu solusinya adalah dengan menggunakan metode kriptografi untuk menanggulangi masalah keamanan dan privasi dari data tersebut.

Kriptografi telah digunakan selama bertahun-tahun dengan tujuan untuk membuat informasi penting hanya terbaca untuk penerima informasi (Zaru & Khan, 2018). Pabokory (2015), menyatakan bahwa kriptografi merupakan seni dan ilmu dalam mengamankan pengiriman data dengan mengubahnya menjadi kode tertentu dan ditujukan hanya untuk pihak tertentu yang memiliki kode atau kunci untuk mengubah kembali kode yang diterimanya yang berfungsi untuk mengembalikan data ke bentuk data asli sebelum dienkripsi. Kriptografi memiliki dua konsep utama yaitu enkripsi dan dekripsi data, enkripsi merupakan proses penyembunyian data sehingga tidak dikenali pihak luar, sedangkan dekripsi merupakan proses mengembalikan data yang telah dienkripsi menjadi bentuk aslinya.

Terdapat banyak algoritma dalam kriptografi, menurut Pramanik (2014) algortima yang menggunakan metode enkripsi transposisi akan menghasilkan *ciphertext* yang aman dan sulit untuk dipecahkan, salah satu algoritma yang menggunakan metode enkripsi transposisi adalah algortima *rail fence*. Oleh karena itu pada penelitian ini akan mengimplementasikan algoritma tranposisi *rail fence* untuk mengamankan data digital.

1.2 Identifikasi Masalah

Berdasarkan penjabaran latar belakang yang telah diapaprkan, maka dapat diidentifikasi masalah dalam penelitian ini adalah sebagai berikut :

1. Pengamanan data digital sangat diperlukan untuk menjaga kerahasiaan data.
2. Diperlukan sistem yang dapat mengamankan data digital.
3. Diperlukan teknik untuk mengamankan data digital yaitu dengan menggunakan algoritma kriptografi *rail fence*.

1.3 Batasan Masalah

Supaya pembahasan dalam penelitian yang dilakukan lebih fokus, maka pembuatan sistem pengaman teks ujian ini akan diberikan batsan masalah sebagai berikut :

1. Sistem ini dikembangkan dengan menggunakan perangkat lunak *Sublime Text 3*, dan *XAMPP*.
2. Karakter yang digunakan dalam pesan adalah karakter yang sesuai dengan standar ASCII.
3. Data yang akan diamankan adalah data yang berupa teks ujian.
4. Algoritma enkripsi yang akan digunakan adalah algoritma *rail fence*.
5. Hasil akhir sistem berupa halaman website dengan data soal ujian yang sudah diproses dengan algoritma enkripsi.

1.4 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka muncul rumusan masalah sebagai berikut:

1. Bagaimana mengamankan data digital teks ujian menggunakan algoritma kriptografi *rail fence*?
2. Bagaimana membangun sistem yang dapat mengamankan data digital berdasarkan teknik pengaman data yang dikembangkan pada penelitian ini?

1.5 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Mengamankan data digital teks ujian menggunakan algoritma *rail fence* sehingga dapat menanggulangi ancaman dan kelemahan terkait keamanan data digital.
2. Membangun aplikasi yang dapat mengamankan data digital teks ujian berdasarkan teknik pengamanan data yang dikembangkan pada penelitian ini.

1.6 Manfaat Penelitian

Manfaat penelitian ini di antaranya:

1. Penelitian ini diharapkan dapat memberikan sumbangan pemikiran serta informasi ilmiah bagi mahasiswa dan masyarakat tentang implementasi algoritma enkripsi *rail fence* untuk mengamankan data digital teks ujian.

2. Dapat melakukan penyembunyian teks ujian, sehingga dapat mengurangi resiko ancaman keamanan yang dapat terjadi.
3. Menghasilkan sistem pengaman teks ujian berbasis website dengan menggunakan algoritma enkripsi *rail fence*.

1.7 Sistematika Penulisan

Laporan penelitian ini disusun dengan menggunakan sistematika sebagai berikut:

BAB I Pendahuluan, terdiri atas latar belakang, identifikasi masalah, batasan masalah, rumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan laporan.

BAB II Kajian Pustaka dan Landasan Teori, berisi tentang teori-teori penunjang yang terkait dengan penelitian ini, antara lain teori mengenai algoritma kriptografi *rail fence*.

BAB III Metode Penelitian, berisi tentang langkah-langkah yang dilakukan dalam penelitian, meliputi identifikasi masalah, studi pustaka, analisis kebutuhan, pemodelan dan pembuatan sistem, pengujian, dan analisis.

BAB IV Hasil dan Pembahasan, berisi tentang hasil implementasi algoritma enkripsi untuk mengamankan teks ujian berserta pembahasannya.

BAB V Kesimpulan dan Saran, berisi tentang kesimpulan dari penelitian yang dilakukan dan saran yang dapat digunakan dalam penelitian selanjutnya

BAB II

KAJIAN PUSTAKA DAN LANDASAN TEORI

2.1 Kajian Penelitian yang Relevan

Choubey & Hashmi (2018) dalam penelitiannya menyatakan bahwa "Cryptography is a science by which we can design strong encryption by applying complex mathematics. Attaining strong encryption means data hiding by which we can hide the secret data which can‟t be permitted by any third person for decryption. So, The art of cryptography also considered as an art of writing where the transfer of secret data can be safely reached to the recipient.", artinya kriptografi adalah ilmu dimana kita dapat merancang sebuah enkripsi yang kuat dengan menerapkan perhitungan yang kompleks. Sebuah enkripsi yang kuat artinya menyembunyikan data dimana data rahasia yang tersembunyi tersebut tidak dapat diakses oleh pihak ketiga untuk dideskripsi. Seni kriptografi juga dianggap sebagai seni menulis dimana trasfer "data rahasia" dapat terkirim pada penerima secara aman.

Penggunaan algoritma *rail fence* dalam enkripsi teks terdapat dalam beberapa penelitian seperti pada Krishna, et al. (2016) yang menggunakan enkripsi kunci simentris dengan algoritma *rail fence* yang men-enkripsi dua pesan dan membuat panjang *cipher text* menjadi setengah dari *plain text*, membuat pengiriman pesan lebih cepat dan aman. Kemudian pada penelitian Siahaan (2016) yang menjelaskan bahwa algoritma *rail fence* merupakan teknik kriptografi yang lebih tinggi dari algoritma *caesar cipher*, dalam penelitian ini juga dijelaskan tahap-tahap enkripsi dan dekripsi pesan menggunakan algortima *rail fence*. Dalam

kesimpulannya Siahaan menyebutkan bahwa untuk memperkuat keamanan enkripsi direkomendasikan untuk menggabungkan algoritma ini dengan algoritma yang lainnya.

Pada penelitian lainnya Prabhakaran & Arumugam (2013) menyatakan bahwa masalah utama dari *cloud computing* adalah privasi data, keamanan, pencurian data dan lain sebagainya. Untuk itu mereka membuat sebuah solusi dengan menggabungkan algortima *rail fence* dan algoritma *caesar* untuk mengamankan data pada *cloud computing* yang mendukung enkripsi data menggunakan 256 ASCII karakter. Penggunaan algoritma enkripsi *caesar cipher* yang diperkuat dengan algoritma *rail fence* juga terdapat pada penelitian Singh, et al. (2012). Singh menyatakan bahwa algoritma *caesar cipher* jika digabungkan dengan algoritma *rail fence* akan meningkatkan keamanan data digital terutama yang berupa data teks digital. Penelitian lainnya oleh Arudchelvam & Fernando (2016) membuat sebuah aplikasi android yang menerapkan algoritma kriptografi *rail fence* dan beberapa algortima lain untuk mengamankan pesan. Pada aplikasi tersebut penerima dan pengirim pesan saling berbagi kunci rahasia yang digunakan untuk mengunci dan membuka isi pesan. Pengamanan pada pengiriman pesan juga telah dilakukan pada penelitian lain (Arfriandi, 2018) yang mengamankan teks pada dokumen email menggunakan metode enkripsi rotor.

Berdasarkan penelitian-penelitian yang telah diuraikan tersebut, penulis akan menerapkan algortima kriptografi *rail fence* untuk mengamankan data digital. Data digital yang akan diamanakan di sini adalah teks ujian, yang nantinya akan disimpan *database* dan sistem yang dihasilkan adalah berbasis website.

2.2 Landasan Teori

2.2.1 Algortima

Ditinjau dari asal usul kata, algortima mempunyai sejarah yang cukup unik. Para ahli hanya menemukan kata *algorism* yang berarti proses menghitung dengan angka arab dan seseorang dapat disebut sebagai *algorist* jika dapat melakukan perhitungan *algorism*. Para ahli bahasa berusaha menemukan asal kata ini namun belum mendapatkan hasil yang memuaskan. Hingga pada akhirnya para ahli sejarah matematika menemukan bahwa kata ini berasal dari seorang penulis buku Arab terkenal bernama Abu Ja'far Muhammad Ibnu Musa Al-Khuwarizmi. Ibnu Musa menulis sebuah buku berjudul Kitab Aljabar Walmuwabala yang berarti Buku Pemugaran dan Pengurangan (*The Book of Restoration dan Reduction*). Dari judul buku tersebut akhirnya ditemukan akar kata Aljabar (*Algebro*).

Karena kata *algorism* sering dikelirukan dengan *arithmetic* maka dilakukan perubahan kata *algorism* menjadi kata *algortihm*, yang mengubah akhiran "*sm*" menjadi "*thm*". Adapun perhitungan dengan angka arab telah menjadi hal biasa, sehingga kata *algortihm* berangsur-angsur digunakan sebagai metode perhitungan (komputasi) dan kehilangan makna kata aslinya. Sedangkan dalam bahasa Indonesia sendiri *algorithm* diserap menjadi kata algortima.

Algortima merupakan langkah-langkah penyelesaian masalah yang tersusun secara sistematik dan logis. Kata logis menjadi kunci dalam algoritma karena langkah-langkah dalam menyelesaikan sebuah algoritma harus logis dan harus bisa ditentukan apakah bernilai benar atau salah (Nurdin, 2017).

2.2.2 Kriptografi

2.2.1.1 Definisi Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani "*cryptos*" yang berarti rahasia, dan "*graphein*" yang berarti tulisan. Oleh sebab itu kriptografi dapat diartikan sebagai tulisan rahasia. Terdapat beberapa definisi kriptografi dalam berbagai sumber. Definisi literatur pada tahun 80-an menyebutkan bahwa kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Seni dalam definisi ini berasal dari fakta sejarah dimana pada awal sejarah kriptografi, setiap orang mempunyai cara yang unik untuk merahasiakan pesan (Nurdin, 2017).

Sedangkan definisi terbaru menyatakan bahwa kriptografi merupakan ilmu mengenai teknik untuk mengirimkan pesan secara rahasia sehingga hanya penerima pesan yang dimaksud yang dapat menghapus, membaca, atau memahami isi pesan tersebut. Definisi lain dari kriptografi yaitu ilmu yang mempelajari metode-metode matematika yang berhubungan dengan aspek keamanan informasi seperti integritas, kerahasiaan, serta otentikasi data (Nurdin, 2017).

Dengan demikian, kriptografi adalah suatu ilmu sekaligus seni yang memiliki tujuan untuk menjaga keamanan sebuah pesan (*cryptography is the art and science of keeping messages secure*). Secara umum, kriptografi adalah teknik pengamanan informasi dimana informasi diubah dengan kunci tertentu melalui enkripsi dan menjadikan informasi ke dalam suatu bentuk informasi baru yang tidak dapat dipahami ataupun dibaca oleh orang yang tidak berhak menerima pesan tersebut, dan informasi tersebut hanya dapat diubah kembali menjadi informasi

semula oleh orang yang berhak menerimanya melalui proses dekripsi (Nurdin, 2017).

2.2.1.2 Sejarah Kriptografi

Kriptografi berawal pertama kali dengan metode pertukaran posisi untuk mengenkripsi suatu pesan tertentu. Kemudian dalam perkembangannya, dikatakan bahwa Julius Caesar dalam mengirim pesan selalu mengacak pesan tersebut sebelum kemudian diberikan kepada para kurir. Karena itu ada pendapat yang menyatakan bahwa Julius Caesar merupakan orang yang mengawali penggunaan kriptografi. Walaupun sebenarnya kriptografi telah digunakan untuk pertama kalinya oleh bangsa Mesir pada 400 tahun lalu dan masih digunakan hingga saat ini.

Kini kriptografi masih diperbincangkan secara luas karena kriptografi dapat digunakan sebagai suatu media untuk melindungi kerahasiaan dan strategi negara. Sejarah kriptografi sebagian besar merupakan kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau dengan bantuan alat mekanik sederhana.

Secara umum algoritma kriptografi klasik dikelompokkan dalam dua kategori, yaitu *transposition cipher* dan *subtitution cipher*. *Transposition cipher* adalah algoritma kriptografi yang mengubah susunan huruf-huruf ataupun karakter yang ada dalam pesan, sedangkan *subtitution cipher* adalah algortima yang mengganti setiap huruf atau kartaker yang terdapat dalam pesan dengan huruf atau kelompok huruf lain.

Kriptografi klasik mencatat penggunaan algoritma *transposition cipher* oleh tentara Sparta pada awal tahun 400 SM di Yunani yang menggunakan suatu alat bernama *scytale* yang terdiri dari sebuah kertas panjang dari daun *papyrus* yang dililitkan pada sebuah silinder dengan diameter tertentu yang berisi kunci penyandian pesan. Kemudian pesan ditulis secara horizontal, baris per baris. Bila pita dilepaskan, huruf-huruf yang ada didalamnya akan tersusun secara acak membentuk pesan rahasia. Untuk membaca pesan yang teracak tersebut, penerima pesan harus melilitkan kembali kertas tersebut pada silinder berdiameter sama dengan diameter silinder pengirim.

Penggunaan *substitution cipher* yang paling awal dan paling sederhana adalah Caesar Cipher yang digunakan raja Yunani kuno, yaitu Julius Caesar. Metode kriptogrrafi yang digunakan adalah dengan mengganti setiap karakter dalam alphabet dengan karakter yang terletak pada tiga posisi berikutnya dalam susunan alphabet yang digunakan.

Pada masa awal agama Kristen, kalangan gereja juga menggunakan kriptografi untuk menjaga tulisan religius yang ada dari gangguan otoritas politik atau budaya yang dominan berkuasa pada saat itu. Metode yang terkenal pada saat itu adalah Angka si Buruk Rupa (*Number of the beast*) yang ada dalam Kitab Perjanjian Baru, yaitu angka “666”. Angka ini menyatakan cara kriptografi untuk menyembunyikan pesan yang dipandang berbahaya. Para ahli percaya bahwa pesan ini mengacu pada Kerajaan Romawi.

Pada abad ke-20 kriptografi lebih banyak digunakan kalangan militer. Pada perang dunia II, Nazi Jerman membuat mesin enkripsi bernama *enigma* yang

menggunakan beberapa *rotor* (roda berputar) dan melakukan enkripsi yang sangat rumit. Nazi Jerman percaya bahwa pesan yang dikirim melalui *enigma* tidak terpecahkan. Tetapi anggapan ini salah karena setelah bertahun-tahun mempelajari mesin *enigma*, pihak Sekutu berhasil memecahkannya. Saat Nazi Jerman mengetahui kode mereka telah terpecahkan, mereka membuat beberapa kali perubahan pada mesin *enigma* (Nurdin, 2017).

2.2.1.3 Manfaat Kriptografi

Menurut Munir (2004) kriptografi memiliki beberapa aspek dalam tujuannya untuk memberikan layanan keamanan. Aspek-aspek tersebut adalah sebagai berikut:

a. Kerahasiaan (*confidentiality*), yaitu layanan yang digunakan untuk menjaga isi pesan dari siapapun yang berhak untuk membacanya.
b. Otentikasi (*authentication*), adalah layanan yang berguna untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan untuk mengidentifikasi kebenaran sumber pesan (*data origin authentication*). “Apakah pesan yang diteriam benar-benar berasal dari pengirim yang benar?”.
c. Integritas data (*data integrity*), merupakan layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. “apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?”.
d. Nirpenyangkalan (*non-repudiation*), layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengiriman pesan

menyangkal melakukan pengiriman atau penerima pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.2.1.4 Istilah dan Konsep dalam Kriptografi

Dalam kriptografi terdapat beberapa istilah atau terminologi yang biasa digunakan (Munir, 2004) diantaranya sebagai berikut:

a. *Plaintext* dan *Ciphertext*

Plaintext (pesan) merupakan data/informasi yang dipahami maknanya. Pesan dapat dikirim atau disimpan dalam media penyimpanan. Agar pesan tidak dapat dipahami oleh pihak yang tidak berkepentingan, pesan perlu disandikan ke dalam bentuk yang tidak dapat dipahami yang disebut *ciphertext*.

b. Peserta Komunikasi

Komunikasi data melibatkan pertukaran pesan minimal yaitu dua entitas. Entitas pertama adalah pengirim yang mengirim pesan kepada entitas lainnya. Entitas kedua adalah penerima yang menerima pesan tersebut. Entitas-entitas ini dapat berupa orang, mesin (komputer), kartu kredit, dan lain sebagainya.

c. Enkripsi dan Dekripsi

Penyandian pesan dari *plaintext* ke *ciphertext* dinamakan enkripsi, sedangkan mengembalikan pesan dari *ciphertext* ke *plaintext* dinamakan dekripsi. Enkripsi dan dekripsi dapat diterapkan pada pesan yang dikirim dan yang disimpan.

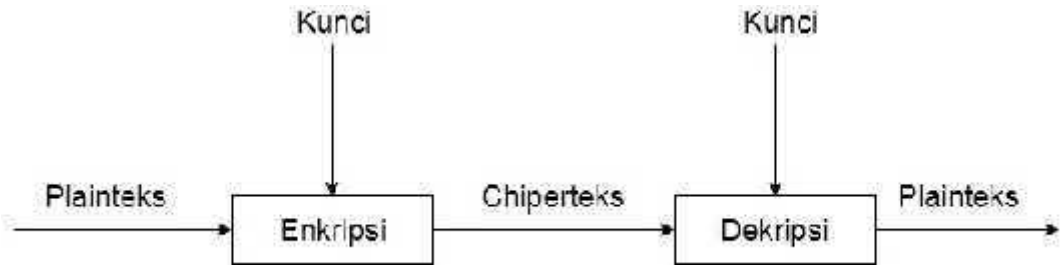
d. Kriptanalis dan Kriptologi

Kriptografi selalu berkembang karena memiliki ilmu yang berlawanan, yaitu kriptanalisis. Kriptografi adalah ilmu dan seni memecahkan *ciphertext* menjadi *plaintext* tanpa memerlukan kunci dan pelakunya disebut kriptanalis. Kriptografer mentransformasikan *plaintext* ke *ciphertext* dengan kunci, sebaliknya kriptanalis memecahkan *ciphertext* untuk menemukan *plaintext* tanpa kunci. Jadi, kriptologi adalah studi mengenai kriptografi dan kriptanalis.

2.2.1.5 Jenis-Jenis Kriptografi

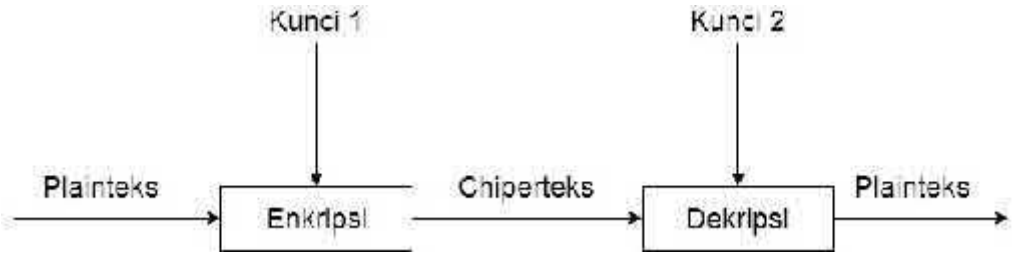
Berdasarkan jenis kunci yang digunakan dalam proses kriptografi, terdapat dua macam kriptografi, yaitu kriptografi simetri dan kriptografi asimetri.

a. Kriptografi simetri, yaitu apabila kunci enkripsi menggunakan kunci yang sama dengan kunci dekripsi. Kriptografi simetri disebut juga dengan kriptografi konvensional. Contoh algoritma simetri adalah *Data Encryption Standard (DES*).



Gambar 2.1. Kriptografi Simetri (Munir, 2004)

b. Kriptografi asimetri, yaitu apabila kunci enkripsi menggunakan kunci yang berbeda dengan kunci dekripsi. Kriptografi asimetri disebut juga dengan kriptografi kunci publik. Contoh algoritma kriptografi asimetri *Rivest-Shamir-Adleman (RSA*).

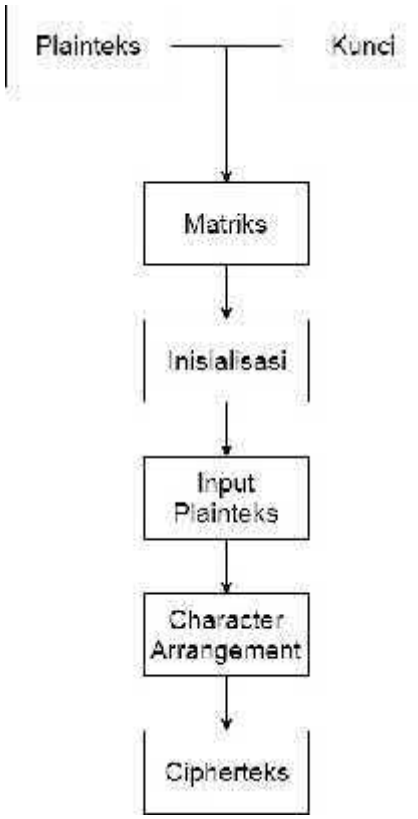


Gambar 2.2. Kriptografi Asimetri (Munir, 2004)

2.3 Algortima *Rail Fence*

Algoritma *rail fence* merupakan algoritma kriptografi kunci simetri yang menggunakan metode transposisi. Cara kerja dari metode transposisi yaitu dengan menyusun ulang posisi masing-masing karakter pada pesan atau *plaintext* sehingga didapatkan suatu hasil enkripsi yang berbeda dari pesan aslinya. Algoritma *rail fence* sering pula dikenal dengan algoritma kriptografi zig-zag, karena pada algoritma *rail fence* karakter pada pesan akan disusun ulang dengan cara membuat lintasan secara zig-zag. Kunci dari metode ini adalah seberapa banyak baris yang digunakan untuk melakukan proses enkripsi dan dekripsi. Baris yang digunakan harus lebih dari satu baris.

Berdasarkan *source code* yang dibuat oleh penulis, Gambar 2.3 adalah struktur program yang merepresentasikan algoritma enkripsi *rail fence*.



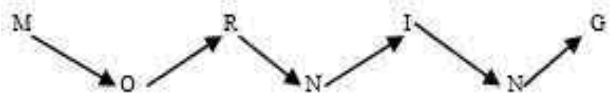
Gambar 2.3. Struktur Program Algoritma *Rail Fence*

Pada awalnya program akan membaca jumlah karakter dari plainteks dan jumlah kunci yang digunakan. Kemudian dibentuklah matriks dengan kolom matriks sesuai jumlah plainteks dan baris matriks sesuai dengan jumlah kunci. Setelah matriks terbentuk, seluruh kolom akan diisi dengan diinisialisasi dengan tanpa karakter. Selanjutnya, karakter plainteks dimasukkan satu per satu pada matriks, dimulai dari kolom pertama baris pertama, kolom kedua baris kedua, dan seterusnya. Jika koordinat matrik mencapai baris terakhir, maka baris yang diisi karakter selanjutnya adalah baris sebelumnya, dengan demikian pengisian karakter akan berurutan secara zig-zag. Dari sini, seluruh karakter pada matiks mulai disusun

ulang, di urutkan dari baris paling atas ke arah kanan, yaitu baris pertama kolom pertama ke kolom selanjutnya, dilanjutkan dengan baris kedua, ketiga dan seterusnya sehingga diperoleh cipherteks yang sulit terbaca.

Langkah-langkah yang perlu dilakukan untuk mengenkripsi pesan dalam algoritma *rail fence* (Saini, 2015) adalah sebagai berikut:

a. Misalkan pesan yang akan dienkripsi adalah MORNING, dengan menggunakan kunci dua baris.
b. Pesan atau *plaintext* ditulis secara berurutan dengan bentuk diagonal.



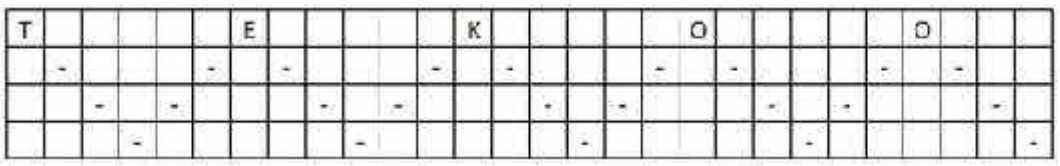
Gambar 2.4. Contoh Algoritma *Rail Fence*

c. Untuk mendapatkan hasil enkripsi, karakter ditulis secara berurutan dari kiri ke kanan dimulai dari baris yang paling atas. Sehingga diperoleh *ciphertext* yaitu MRIGONN.

Langkah-langkah dalam dekripsi *ciphertext* dari algortima *rail fence* (Clark, n.d.) adalah sebagai berikut:

a. Misalkan pesan yang akan dienkripsi adalah TEKOOHRACIRMN-REATANFTETYTGHH dengan jumlah 4 baris (kunci) dan panjang 28 kolom (banyak karakter).

b. Letakkan “T” pada kotak pertama. Kemudian beri tanda garis pada kotak selanjutnya di bawahnya secara diagonal sampai kembali pada baris teratas, dan letakkan karakter “E”. Lanjutkan hingga baris pertama mendapatkan pola seperti Gambar 2.5.



Gambar 2.5. Tahap Pertama Proses Dekripsi

c. Lanjutkan cara ini baris demi baris, dan akan diperoleh hasil seperti Gambar 2.8.

Gambar 2.6. Tahap Kedua Proses Dekripsi

Gambar 2.7. Tahap Ketiga Proses Dekripsi

Gambar 2.8. Tahap Keempat Proses Dekripsi

d. Dari Gambar 2.8 didapatkan sebuah pesan yang dapat dibaca secara diagonal yaitu “THEY ARE ATTACKING FROM THE NORTH”.

BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Dari hasil implementasi dan pengujian yang telah dilakukan, diperoleh kesimpulan sebagai berikut:

a. Aplikasi dapat digunakan untuk mengenkripsi teks ujian dan menyimpannya pada *database*. Pesan yang telah tersimpan pada *database* dapat diketahui kembali secara utuh melalui proses dekripsi.

b. Berdasarkan hasil uji *white-box*, implementasi algoritma kriptografi *rail fence* memperoleh hasil yang memuaskan pada pengujian algoritma enkripsi dan dekripsi yang artinya sistem dinyatakan valid dan dapat berjalan dengan baik untuk mengamankan data teks ujian.

5.2 Saran

Berdasarkan penelitian yang dilakukan, terdapat beberapa saran yang dapat digunakan untuk penelitian selanjutnya, antara lain:

a. Menggabungkan algoritma kriptografi *rail fence* dengan algoritma lain dalam mengamankan data. Sehingga meningkatkan keamanan algoritma enkripsi menjadi lebih rumit dan sulit untuk dipecahkan.

b. Sistem yang telah dibuat ini merupakan sistem pengamanan dan penyimpanan teks ujian, penelitian selanjutnya diharapkan dapat mengembangkan sistem agar dapat digunakan pada ujian secara langsung.

DAFTAR PUSTAKA

Arfriandi, A., 2018. Pengamanan Teks Pada Dokumen Email Menggunakan Enkripsi Rotor. *Edu Komputika Journal,* Volume 5, pp. 23-32.

Arudchelvam, T. & Fernando, W. W. E. N., 2016. Maintaining User-Level Security in Short Message Service. *International Journal of Computer, Electrical, Automation, Control and Information Engineering,* pp. 997-1000.

Choubey, R. K. & Hashmi, A., 2018. Cryptographic Techniques in Information Security. pp. 854-859.

Clark, D. R., t.thn. *Rail Fence Chiper - Crypto Corner.* [Online] Available at: http://crypto.interactive-maths.com/rail-fence-cipher.html [Diakses 19 08 2018].

Floyd, T., Grieco, M. & Reid, E. F., 2016. Mining Hospital Data Breach Records: Cyber Threats to U.S. Hospitals. pp. 43-48.

Hastaka, A. Y., 2017. *PENGAMANAN SOAL UJIAN SEKOLAH DENGAN ALGORITMA KRIPTOGRAFI ADVANCE ENCRYPTION STANDARD (AES) DAN METODE STEGANOGRAFI END OF FILE (EOF) PADA SMA NEGERI 1 WELERI,* s.l.: s.n.

Khan, M. E., 2011. Different Approaches to White Box Testing Technique for Finding Errors. *International Journal of Software Engineering and Its Applications,* Volume 5, pp. 1-14.

Knight, S., 2010. *The Rail Fence Cipher.* [Online] Available at: http://www.cs.trincoll.edu/~crypto/historical/railfence.html [Diakses 4 11 2018].

Krishna, B. H., Kiran, D. S., Reddy, I. R. S. & Reddy, R. P. K., 2016. Multiple text encryption, Key entrenched, distributed cipher using pairing functions and transposition ciphers. *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016,* pp. 1059-1061.

Munir, R., 2004. Pengantar Kriptografi. *Departemen Teknik Informatika Institut Teknologi Bandung,* Issue Bahan Kuliah, p. 12.

Nurdin, A. P. N., 2017. ANALISA DAN IMPLEMENTASI KRIPTOGRAFI PADA PESAN RAHASIA MENGGUNAKAN ALGORITMA CIPHER TRANSPOSITION. *Jesik,* Volume 3, pp. 1-11.

Pabokory, F. N., Astuti, I. F. & Kridalaksana, A. H., 2015. Implementasi Kriptografi Pengaman Data. *Jurnal Informatika Mulawarman,* pp. 20-31.

Patelia, R. M. & Vyas, S., 2014. Review and Analysis on Cyclomatic Complexity. *ORIENTAL JOURNAL OF COMPUTER SCIENCE & TECHNOLOGY,* Volume 7, pp. 382-384.

Ponemon Institute LLC, 2018. *2018 Cost of Data Breach Study, Global Overview*. s.l.:s.n.

Prabhakaran, S. & Arumugam, P., 2013. Multilevel Encryption for Ensuring Public Cloud. *International Journal of Advanced Research in Computer Science and Software Engineering,* pp. 402-405.

Pramanik, M. B., 2014. Implementation of Cryptography Technique using Columnar Transposition. *International Journal of Computer Applications,* pp. 19-23.

Randive, R. B. & Bansode, S. Y., 2017. White Box Testing with Object Oriented programming. *International Journal of Recent Trends in Engineering and Research,* 3(11), pp. 156-160.

Saini, B., 2015. Modified Ceaser Cipher and Rail fence Technique to Enhance Security. *International Journal of Trend in Research and Development,* 2(5), pp. 348-350.

Siahaan, A. P. U., 2016. Rail Fence Cryptography in Securing Information. *International Journal of Scientific & Engineering Research,* 7(7), pp. 535-538.

Singh, A., Nandal, A. & Malik, S., 2012. Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security. *International Journal of Advanced Research in Computer Science and Software Engineering,* 2(12), pp. 78-82.

Sugiyono, 2015. *Metode penelitian pendidikan:(pendekatan kuantitatif, kualitatif dan R & D).* s.l.:Alfabeta.

Zaru, A. & Khan, M., 2018. General Summary of Cryptography. *Int. Journal of Engineering Research and Application,* pp. 68-71.