**PENERAPAN KEAMANAN FILE MENGGUNAKAN ALGORITMA BASE64 DAN AES (ADVANCED ENCRYPTION STANDART )**

Dosen Pembimbing : TEGUH TAMRIN, S.Kom, M.Kom.

A picture containing chart

Description automatically generated

Disusun Oleh :

Ahmad Suroyya Mutsaddad

(191240000937)

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS SAINS DAN TEKNOLOGI**

**UNIVERSITAS ISLAM NAHDLATUL ULAMA JEPARA**

**2022**

# PERSETUJUAN PEMBIMBING

# DAFTAR ISI

HALAMAN JUDUL………………………………………………………………i

[PERSETUJUAN PEMBIMBING ii](#_Toc106339550)

[DAFTAR ISI iii](#_Toc106339551)

[DAFTAR GAMBAR iv](#_Toc106339552)

BAB I [PENDAHULUAN 1](#_Toc106339554)

[1.1 Latar Belakang 1](#_Toc106339555)

[1.2 Perumusan Masalah 5](#_Toc106339556)

[1.3 Batasan Penelitian 5](#_Toc106339557)

[1.4 Tujuan Penelitian 5](#_Toc106339558)

[1.5 Manfaat Penelitian 5](#_Toc106339559)

[1.6 Sistematika Penulisan 6](#_Toc106339560)

BAB II [LANDASAN TEORI 8](#_Toc106339562)

[2.1. Tinjauan Studi 8](#_Toc106339563)

[2.2. Tinjauan Pustaka 10](#_Toc106339564)

[2.2.1 Keamanan Informasi 10](#_Toc106339565)

[2.2.2 Pertukaran Informasi 10](#_Toc106339566)

[2.2.3 Ancaman Informasi 11](#_Toc106339567)

[2.2.5 Enkripsi 14](#_Toc106339568)

[2.2.6 Dekripsi 14](#_Toc106339569)

[2.2.7 Algoritma Kriptografi 15](#_Toc106339570)

[2.2.8 Algoritma Rail Fence Cipher 17](#_Toc106339571)

[2.2.9 Evaluasi 19](#_Toc106339572)

[2.3. Kerangka Pemikiran 20](#_Toc106339573)

BAB II [METODOLOGI PENELITIAN 21](#_Toc106339575)

[3.1. Gambaran Umum Penerapan Algoritma 21](#_Toc106339576)

[3.2. Flowchart Enkripsi 21](#_Toc106339577)

[3.3. Flowchart Dekripsi 22](#_Toc106339578)

[3.4. Pengujian Penerapan Algoritma 23](#_Toc106339579)

[DAFTAR PUSTAKA 24](#_Toc106339580)

# DAFTAR GAMBAR

**Gambar 2.1.** Diagram Alur Kriptografi 13

**Gambar 2.2.** Diagram proses enkripsi dan dekripsi algoritma simteris 15

**Gambar 2.3.** Diagram proses enkripsi dan dekripsi algoritma asimteris 16

**Gambar 2.4.** Algoritma Rail Fence Cipher 17

**Gambar 3.1.** *Flowchart* enkripsi teks 21

**Gambar 3.2.** *Flowchart* enkripsi teks 22

# BAB I

# PENDAHULUAN

## Latar Belakang

Di zaman teknologi yang semakin berkembang dan maju, orang-orang telah melakukan banyak pengembangan dalam bidang teknologi digital dalam hal pengamanan data secara digital dan pengamanan dokumen secara digital. Keamanan kriptografi bermula dari kebutuhan untuk melindungi pesan rahasia dari orang-orang yang tidak berwenang. Sejarah kriptografi bisa dilacak kembali hingga ribuan tahun yang lalu, ketika orang menggunakan teknik-teknik sederhana seperti penggantian karakter atau penjumlahan numerik untuk menyandikan pesan rahasia. Namun, dengan berkembangnya teknologi komunikasi, metode kriptografi sederhana ini menjadi mudah dibobol oleh orang yang tidak berhak. Oleh karena itu, kriptografi modern menggunakan algoritma matematika yang rumit untuk menyandikan pesan dan melindungi data pribadi. Teknologi tumbuh dalam kecanggihan seiiringnya waktu dan serangan dunia maya yang canggih kriptografi dapat terus berkembang untuk mengatasi ancaman baru. Saat ini, kriptografi modern menghasilkan teknik yang lebih kuat seperti kriptografi kunci publik, kriptografi homomorfik, dan kriptografi kuantum,Kriptografi hanya untuk pengelola data yang bertujuan untuk mengamankan data yang sederhana dan bersifat sementara, tapi setelah terbarukan kriptografi ialah data yang enkripsi serta data dekripsi untuk keamanan [1].

Keamanan dalam kriptografi merupakan isu penting karena informasi sensitif dan pribadi seringkali disimpan dan dikirimkan dalam bentuk digital. Tanpa tindakan pengamanan yang memadai, informasi ini dapat dicuri, dimanipulasi, atau diakses oleh pihak yang tidak berwenang. Salah satu untuk mengatasi cara dalam menjaga isi pesan tersebut dengan dilakukanya sebuah pengubahan pesan dari suatu text maupun file menjadi sandi yang hanya diketahui oleh pengirim dan penerima pesan. Sejarah keamanan kriptografi mencatat beberapa insiden keamanan penting. Salah satu insiden paling terkenal adalah pecahnya mesin Enigma Jerman yang digunakan dalam Perang Dunia II oleh Alan Turing dan timnya. Keberhasilan ini membuka jalan bagi kemenangan Sekutu dalam perang. Meskipun kriptografi terus berkembang, tantangan keamanan tetap ada. Salah satu tantangan utamanya adalah serangan siber yang dapat menembus sistem keamanan dan mengakses informasi sensitif. Serangan dunia maya dapat dilakukan dengan berbagai cara, seperti serangan brute force, serangan phishing, atau serangan man-in-the-middle [2].

Pertukaran informasi adalah salah satu yang sudah dilakukan dalam kehidupan manusia sejak dahulu, yang memungkinkan manusia mendapat informasi dengan manusia lainya. Informasi tersebut dapat dirubah menjadi informasi baru yang berguna untuk manusia sendiri dan untuk orang lain juga. Pada zaman sekarang berbagi informasi tidak hanya secara langsung maupun melalui surat dengan berkembangnya zaman berbagi informasi dapat dilakukan menggunakan aplikasi seperti whatsaap, telegram maupun facebook. Bukan berarti hal tersebut tidak memiliki kekurangan semua sistem digital pasti memliki kekuranganya masing-masing. Informasi pada aplikasi tersebut dapat dengan mudah dilihat oleh orang lain, baik penyedia maupun orang yang berniat dalam melakukan pencurian data maupun informasi yang biasa disebut *hacker.* Hal ini dapat dicegah melalui pihak ketiga dalam pengiriman sebuah file maupun bisa menggunakan kunci untuk membuka informasi yang diterima untuk guna menghindari orang berniat buruk dalam mengetahui informasi untuk keperluan sendiri atau diperjual belikan[3].

Pengubahan teks informasi dilakukan dengan cara teknik yang biasa disebut enkripsi dimana teks asli yang disebut dengan (plaintext) diacak menggunakan suatu kunci yang menghasilkan teks acak yang disebut (chipertext). Dalam kasus enkripsi ada beberapa istilah yaitu enkripsi simteris dengan melakukan pengacakan menggunakan kunci atau key yang sama atau tidak berubah teknik ini dapat mendapat teks asli dengan menggunakan teknik yang sama, enkripsi asimteris dengan melakukan teknik pengacakan dengan pengamanan key atau kunci yang berbeda untuk membukanya dalam kasus penggunaan teknik asimteris kemungkinan kecil dalam pencurian data dengan menggunakan bruteforce.Enkripsi dan dekripsi teks maupun dokumen akan disandikan dengan metode tertentu sehingga kebocoran data infromasi kepada tangan yang tidak berwewenang atau ada kebocoran dalam sistem tidak akan mudah mengetahui isi asli dari pesan teks untuk membuka sebuah dokument yang sudah disandikan. Begitu sebaliknya ketika datat tersebut diterima oleh pengguna asli atau penerima asli dengan mengetahui kunci maka dapat membuka teks sebagai kunci untuk membuka dokument yang diterima[4].

Teknik enkripsi dan dekripsi digunakan untuk mengubah teks menjadi kode-kode tertentu sehingga informasi tersebut tidak dapat dibaca oleh siapapun selain pihak yang berwenang. Metode enkripsi yang umum digunakan adalah algoritma simetris, yang menggunakan kunci yang sama saat melakukan enkripsi dan dekripsi, sehingga informasinya tidak dapat dipahami jika sang pembaca tidak memiliki kunci. Algoritma kriptografi dibagi menjadi algoritma klasik dan algoritma modern. Contoh algoritma klasik adalah cipher pagar kereta api yang saat ini digunakan dalam penelitian ini, sedangkan contoh algoritma modern adalah algoritma Twofish dan Rijndael [5]. Enkripsi adalah proses dimana informasi (teks) atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali (acak), sedangkan Dekripsi adalah mengubah kembali dari bentuk yang tidak dikenali tersebut menjadi informasi (teks) awal[6].

Tujuan dari kriptografi adalah untuk mendapatkan kerahasiaan dan keaslian dari semua sumber informasi. Kriptografi tidak hanya melindungi data dari pencurian atau mengubah pesan, tetapi juga dapat digunakan untuk mengautentikasi pengguna. Ada beberapa istilah dalam kriptografi, antara lain: kode disebut cipher, informasi atau teks yang disembunyikan disebut plaintext, dan teks yang dikirim setelah mengubah informasi menjadi bentuk rahasia disebut ciphertext. Proses dari plaintext menjadi ciphertext disebut enkripsi, dan proses dari ciphertext menjadi plaintext disebut dekripsi.

Algoritma base64 sangat baik untuk digunakan dalam mengacak teks. Karakter-karakter pada plaintext akan ditransposisikan ke tempat lain sehingga plaintext tersebut tidak dapat difahami oleh orang lain. Dengan menerapkan algoritma ini, data akan terjamin kerahasiaannya. Metode ini sangat cepat dalam operasinya. Untuk melakukan ini, algoritma Base64 membagi setiap blok 3-byte data biner menjadi 4 grup 6 bit, dan kemudian mengubah setiap grup 6 bit menjadi 1 karakter ASCII pesan sehingga pesan pun dapat diacak menggunakan kata-kata yang ada pada pesan tersebut. Semakin banyak kata-kata pada pesan tersebut, maka hasil ciphertext akan semakin kuat untuk diretas oleh seseorang yang ingin mencuri pesan tersebut. Metode Base64 mengelompokkan setiap blok data biner ke dalam kelompok-kelompok 6 bit. Kemudian, setiap kelompok 6 bit tersebut diubah menjadi 1 karakter ASCII menggunakan tabel karakter Base64 yang telah ditentukan[7]. Advanced Encryption Standard (AES) sebuah algoritma kriptografi simetris yang digunakan untuk mengenkripsi dan mendekripsi data. Algoritma AES dikenal juga dengan nama Rijndael, yang diusulkan oleh dua ahli kriptografi Belgia, Vincent Rijmen dan Joan Daemen. AES menggunakan sebuah kunci rahasia yang sama untuk mengenkripsi dan mendekripsi data[8].

Dengan adanya permasalahan kemanan pada melakukan pertukaran data dan informasi berbasis sebuah file solusi dalam menangani tersebut dengan adanya kombinasi dalam sebuah penerapan algoritma untuk melakukan enkripsi sehingga kemungkinan dalam terjadinya kebocoran data menggunakan kombinasi antara base64 dan AES(Advanced Encryption Standart) kemungkinan kecil terjadinya kebocoran sebuah sebuah informasi. Dikarenakan metode ini dalam tahap proses penulisan kita perlu mengubah sebuah kedalam format ASCII dengan hasil chipertext base64 tadi di enkrip lagi menggunakan Algoritma AES dengan kunci yang sudah ditentukan sehingga menambah kerumitan dalam melakukan enkripsi dan dekripsi.

## Perumusan Masalah

Berdasarkan latar belakang masalah diatas maka perumusan masalah dalam penelitian ini adalah bagaimana mengamankan pertukaran informasi berupa file memanfaatkan teknik kriptografi?

## Batasan Penelitian

Adapun batasan penelitian dalam pengerjaan penelitian ini

adalah sebegai berikut :

1. Metode yang digunakan dalam penelitian adalah metode base64 dan AES (Advanced Encryption Standart).
2. Data yang digunakan dalam enkripsi hanya file berformat pdf.
3. Data diambil dari data file pdf.
4. Penelitian ini tidak menerapkan penyandian dalam aplikasi tertentu.
5. Pengujian / penerapan tidak mempertimbangkan jaringan internet.

## Tujuan Penelitian

Berdasarkan perumusan masalah diatas maka tujuan penelitian dalam penelitian ini adalah menerapkan metode base64 dan AES(Advanced Encryption Standart) untuk mengamankan pertukaran informasi menggunakan data file.

## Manfaat Penelitian

Dari penelitian diatas diharapkan dapat memberikan manfaat sebagai berikut :

1. Manfaat bagi peneliti

Adapun manfaat bagi peneliti yaitu menambah ilmu pengetahuan khususnya pada keamanan dalam menggunakan algortima kriptografi.

1. Manfaat bagi pengirim dan penerima pesan

Pengirim dan penerima pesan dapat menyandi file agar lebih aman saat berkomunikasi.

1. Manfaat bagi pembaca

Dapat menambah wawasan bagi pembaca dan dapat dipergunakan sebagai referensi untuk penelitian selanjutnya.

1. Manfaat bagi keamanan informasi

Dapat menjaga keamanan dalam bertukar informasi dengan menerapkan metode lebih 1 algoritma base64 dan AES (Advanced Encryption Standart).

## Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab ini membahas tentang latar belakang, rumusan masalah, batasan penelitian , tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi mengenai tinjauan studi, tinjuan pustaka, dan kerangka pemikiran.

BAB III METODOLOGI PENELITIAN

Pada bab ini mejelaskan tentang kerangka penelitian, lokasi penelitian, desain penelitian, pengumpulan data, metode pengembangan sistem, dan pengujian metode.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini mejelaskan tentang penerapan dari aplikasi tersebut.

BAB V KESIMPULAN DAN SARAN

Pada bab ini mejelaskan tentang kesimpulan dan saran yang diharapkan dapat bermanfaat untuk mengembangkan pembuatan program aplikasi selanjutnya.

# BAB II

# LANDASAN TEORI

## Tinjauan Studi

Penelitian ini merujuk pada beberapa referensi yang telah dilakuka oleh peneliti peneliti sebelumnya untuk dijadikan refererensi sekaligus sebagai sumber bertukar informasi diantaranya:

Penelitian yang dilakukan oleh Tio Lovian, Iskandar Fitri.Pada tahun 2022,dengan judul “Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang”,dalam penelitian ini permasalahan yang dikhawatirkan terjadi pencurian data pada aplikasi pencatat yang dimana aplikasi menyimpan data email password dan data tranksaksi sehingga diterapkanya pengamanan enkripsi pada data guna menghindari kebocoran data yang bersifat penting[9].

Penelitian yang dilakukan Masduki, Aan Suhartana, I Ketut Gde. Pada tahun 2019, dengan judul “Proteksi Aplikasi Pesan SMS Berbasis Mobile Android Dengan Algoritma AES 256 dan Steganografi LSB”, Dalam penelitian ini yang dikhawatirkan adalah data bisa jatuh ke pihak yang salah dan kemudian disalahgunakan untuk hal-hal negatif. Salah satu cara untuk mengatasi masalah tersebut adalah dengan menyandikan pesan text yang dikirim sehingga bentuk pesan sebelum sampai di penerima menjadi acak. Oleh karena itu, jika jatuh ke tangan yang tidak diinginkan, pesan tersebut juga tidak dapat digunakan[10].

Berdasarkan penelitian mengenai Implementasi Algoritma Rail Fence Chiper Dalam Keamanan Data Gambar 2 Dimensi, dalam penelitian ini permasalahan yang dikhawatirkan adalah data tersebut dapat jatuh kepihak yang tidak diinginkan, yang kemudian disalahgunakan untuk hal-hal bersifat negatif. Salah satu cara untuk mengatasi hal tersebut adalah menyandikan citra tersebut sehingga bentuk citra menjadi teracak. Sehingga apabila jatuh ketangan yang tidak diinginkan, citra tersebut juga tidak dapat digunakan[11].

Algoritma Caesar cipher dan rail fence cipher berhasil diterapkan oleh Jannah, Miftah Halul, Khairil, dan Aspriyono, untuk mengatasi permasalahan keamanan dalam pengiriman pesan antara komputer satu ke komputer lain, lalu peneliti membuat sebuah aplikasi untuk meningkatkan keamanan berupa proses enkripsi menggunakan algoritma caesar cipher yang kemudian dienkripsi lagi

menggunakan rail fence cipher. Aplikasi yang dibuat berbasis client sever yang menggunakan bahasa pemrograman Visual Basic.Net dengan database SQL server[12].

Pada artikel yang telah dibuat oleh Simamora, Adi Putra, Haryanto, Edy Victor, Yusfrizal, Kartika, Fani Budi, dan Sianturi, Noprita Elisabeth. Pada tahun 2022, dengan judul “Perancangan Aplikasi Keamanan File PDF Dengan Algoritma Rail Fence + Xor Berbasis Android”, dalam penelitian ini peneliti merancang sebuah aplikasi pada android yang bisa digunakan untuk mengamankan isi pesan pada file pdf dari orang tidak berwenang. Dalam mengamankan file pdf tesebut peneliti menggunakan algoritma rail fence cipher + XOR yang bekerja dalam enkripsi dan dekripsi isi pesan yang ada pada file pdf. Dimana dalam penelitian ini membutuhkan bahasa pemrograman android studio dalam merancang aplikasi keamanan file pdf tersebut[13].

Teknik enkripsi berhasil diterapkan untuk mengamankan data teks, dalam penelitian ini untuk pengamanan data teks menggunakan caesar cipher masih memiliki kelemahan di antaranya jumlah karakter yang terbatas sebanyak 26 karakter. Hal ini yang dapat membuat hasil enkripsi dengan mudah dapat dikenali oleh pihak lain. Penelitian ini bertujuan untuk merancang sebuah usulan dalam menjaga keamanan data melalui teknik kriptografi, sekaligus mengatasi permasalahan yang terdapat pada algoritma caesar cipher. Perpaduan antara algoritma Caesar dan algoritma Beaufort dilakukan untuk mengatasi permasalahan yang ada[14].

Sedangkan penelitian tentang analisa pada pengaman teks menggunakan kriptografi block cipher yang dilakukan oleh Sinawati, Indrianti, dan Hafid, M. Pada tahun 2018 “Analisa Kriptografi Block Cipher Pada Pengamanan Teks Menggunakan Metode Triple Transposition Vigenere Cipher”, masalah pada penelitian ini ketidakseimbangan antara setiap perkembangan suatu teknologi yang tidak diiringi dengan perkembangan pada sistem keamanannya itu sendiri, maka dari itu peneliti melakukan melakukan proteksi terhadap pengamanan teks dengan cara melakukan proses acak teks atau enkripsi, serta melakukan proses pengembalian teks ke bentuk semula atau dekripsi dengan menerapkan algoritma kriptografi block cipher menggunakan metode Triple Transposition Vigenere Cipher[15].

Permasalahan dalam penelitian yang dibuat oleh R M. Abu Jihad Plaza, dan Hartono, R. Pada tahun 2021, “Penerapan Kriptografi Caesar Chiper Pada Aplikasi Chatting Berbasis Local Area Network”, dalam penelitian ini masalah yang diangkat adalah pengguna jaringan komputer sering dihadapkan pada masalah komunikasi antar pengguna. Peneliti membuat sebuah Aplikasi chat digunakan sebagai media komunikasi antar sesama pengguna komputer yang terhubung dalam suatu jaringan, baik melalui teks, gambar, maupun suara yang diimplementasikan ke dalam algoritma *Advanced Encryption Standard* (AES) yang digunakan sebagai algoritma kriptografi standar Caesar Chiper. AES sendiri merupakan algoritma kriptografi dengan menggunakan algoritma caesar chiper yang dapat mengenkripsi dan mendekripsi blok data[16].

Penelitian yang ditulis oleh Maya Sari, Hindriyanto Dwi Purnomo, dan Irwan Sembiring 2022 dengan judul Algoritma Kriptografi Sistem Keamanan SMS di Android, dalam penelitian ini membahas tentang penggunaan smartphone yang luas dimasyarakat. Namun, meskipun teknologi *smartphone* ini memiliki banyak fitur, penggunanya tetap memiliki pertimbangan khusus untuk email SMS (*Short Message Service*). Tetapi SMS ini memiliki keterbatasan, hanya dalam keamanan pertukaran informasi rahasia, sistem ini diperlukan untuk memberikan keamanan pertukaran informasi melalui SMS berbasis Android. Oleh karena itu diperlukan pengamanannya dengan menggunakan metode kriptografi dan diperlukan tingkat keamanan yang tinggi. Pada penelitian ini akan membandingkan tiga algoritma kriptografi yaitu *Advanced Encryption Standard* (AES), Rivest Shamir Adleman, dan Tiny Encryption Algorithm yang dilakukan dengan cara membandingkan karakteristik algoritma enkripsi yang hasilnya akan digunakan untuk sistem keamanan SMS berbasis Android dengan keamanan yang lebih tinggi[17].

## Tinjauan Pustaka

## Keamanan Informasi

Keamanan informasi adalah sekumpulan metode, ataupun proses yang disusun dan diterapkan untuk melindungi informasi atau data pribadi dari penyalahgunaan, gangguan, atau pengubahan yang tidak resmi. Keamanan informasi bertujuan untuk melindungi data pada berbagai tahap, baik itu ketika proses menyimpan, mengirim, atau menggunakannya. Masalah keamanan sering kali kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Seringkali masalah keamanan berada pada urutan setelah tampilan, atau bahkan diurutan terakhir dalam daftar hal- hal yang dianggap penting. Apabila mengganggu performa dari sistem, seringkali masalah keamanan tidak begitu diperhatikan bahkan ditiadakan.

Dengan adanya kemungkinan penyadapan data informasi, maka keamanan dalam pertukaran informasi menjadi sangat penting karena suatu komunikasi jarak jauh belum tentu memiliki jalur yang aman dari penyadapan. Jika ada data-data yang tidak terlalu penting, sehingga apabila publik mengetahui data tersebut, pemilik data informasi tidak terlalu dirugikan. Tetapi apabila Pemilik data informasi adalah pihak militer atau pemerintah, keamanan dalam pertukaran informasi menjadi sangat penting karena data yang mereka kirim kebanyakan adalah data-data rahasia yang tidak boleh diketahui oleh publik. Masalah keamanan merupakan salah satu aspek terpenting dari suatu sistem informasi. Maka dari itu dibutuhkan keamanan informasi menggunakan kriptografi. Algoritma rail fence cipher diimplementasikan untuk melakukan enkripsi dan dekripsi data informasi (teks)[18].

## Pertukaran Informasi

Pertukaran informasi sudah mulai dilakukan sejak tahun 1926 dan terus mengalami perubahan serta penyempurnaan ke arah yang lebih baik. Pertukaran informasi pada awalnya masih memiliki keterbatasan terkait kerahasiaan informasi tetapi sekarang telah dilaksanakan secara otomatis[19]. Hal itu membuat pertukaran informasi menjadi tren pada saat itu, semua orang melakukan kegiatasn bertukar informasi mulai dari bertukar informasi mengenai kabar terkini sampai digunakan sebagai otoritas pajak dalam melakukan *cross check* atas informasi yang telah tersedia**.**

Teknologi informasi merupakan salah satu sarana dan prasarana untuk menyajikan informasi yang berbentuk struktur kelembagaan dan nilai-nilai sosial yang dikumpulkan, disimpan, diolah dan dipertukarkan, sehingga memungkinkan untuk terjadinya persamaan persepsi dan atau tindakan. Informasi saat ini dapat diperoleh melalui media manapun dengan menggunakan internet sekalipun. Tidak hanya media cetak, televisi dan radio, saat ini media elektronik seperti media sosial yang lebih mudah digunakan dengan hanya melalui perangkat komunikasi *mobile phone* seperti *smartphone*. Dalam memenuhi kebutuhan informasi, media sosial merupakan salah satu media yang paling disukai bagi masyarakat. Adanya interaksi dalam media sosial membuat pertukaran informasi lebih bersifat dua arah. Saat ini, media konvensional tidak lagi menjadi pilihan utama. Media sosial adalah sebuah media online berbasis internet yang dibangun atas dasar ideologi dan teknologi Web 2.0[20].

## Ancaman Informasi

Serangan terhadap keamanan sistem informasi ini seringkali terjadi. Kejahatan pada dunia maya seringkali dilakukan oleh sekelompok orang yang ingin menembus suatu keamanan sebuah sistem. Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan. Tidak semua pekerjaaan meretas murni dilakukan dari balik layar atau hanya fokus mengeksploitasi perangkat keras, karena semakin berkembangnya zaman keamanan komputer juga semakin sulit ditembus keamanannya. Teknik ini banyak dipakai untuk penyebaran virus malware atau mendapatkan informasi yang diperlukan peretas, seperti identitas seseorang, dan lain-lain. *Social engineering* merupakan istilah yang digunakan untuk berbagai tindak kejahatan yang dilakukan dengan memanfaatkan interaksi dengan manusia. Teknik ini menggunakan manipulasi psikologis untuk menipu korban agar mereka melakukan kesalahan keamanan dan memberikan informasi sensitif. *Social engineering* sering digunakan oleh para peretas untuk mendapat informasi penting karena mereka memahami bahwa manusia menjadi rantai terlemah pada sistem keamanan jaringan. Meskipun programmer telah membangun sistem keamanan yang baik, namun jika dioperasikan oleh pengguna yang tidak kompeten, sistem tetap bisa dengan mudah diserang oleh peretas[21].

Hal yang harus diperhatikan untuk menjaga dari ancaman informasi adalah :

1. Jaringan

Keamanan jaringan merupakan hal sangat penting untuk diperhatikan terutama di era teknologi sekarang ini, karena banyak instansi yang tidak terlalu memperdulikan adanya masalah keamanan jaringan. Ketika jaringan komputer mendapat serangan virus, spam dan malware maka akan terjadi kerusakan data dan kerusakan sistem yang dapat mengakibatkan kerugian pada perusahaan. Oleh karena itu jaringan internet harus memiliki tingkat keamanan yang tinggi untuk mencegah kerusakan dari ancaman informasi yang beragam[22].

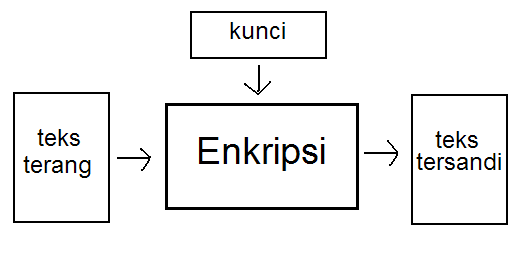
1. Firewall

Untuk itu peran firewall adalah untuk melindungi, mengawasi dan membatasi akses ilegal yang akan masuk kedalam jaringan internal[22].

1. **Kriptografi**

Kriptografi mempunyai peranan penting dalam dunia komputer. Hal ini disebabkan karena banyaknya informasi rahasia yang disimpan dan dikirimkan melalui media-media komputer. Informasi-informasi ini biasanya bersikan dokumen-dokumen penting atau bersifat rahasia dari suatu instansi yang tidak ingin dibaca oleh orang yang tidak berhak atas informasi tersebut. Dengan komputer digital, akan sangat mungkin untuk menghasilkan cipher (teks rahasia) yang lebih kompleks dan rumit. Ada dua jenis kriptografi yaitu klasik dan modern. Kriptografi klasik pada umumnya dienkripsi karakter per karakter (menggunakan alfabet tradisional), sedangkan kriptografi modern beroperasi pada string biner. Dengan kata lain kriptografi klasik dan modern tidak hanya memberikan aspek keamanan, tetapi juga kepada aspek-aspek lain dalam dunia digital. Kriptografi adalah metode untuk mengirim pesan secara rahasia sehingga hanya penerima yang bisa menghapus penyamaran dan membaca pesan atau menguraikannya[23]. Dalam kriptografi sendiri terdapat beberapa istilah, yaitu: Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi:

1. Plaintext (M) adalah pesan yang hendak dikirimkan (berisi data asli).
2. Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
3. Enkripsi (E) adalah proses pengubahan plaintext menjadi ciphertext.
4. Dekripsi (D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal atau asli.
5. Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.



***Gambar 2.1.*** Diagram Alur Kriptografi *(Sumber: https://id.wikipedia.org/wiki/Kunci\_%28kriptografi%29)*

## Enkripsi

Pada kriptografi terdapat teknik yang digunakan untuk mengamankan suatu pertukaran informasi yaitu teknik enkripsi. Enkripsi adalah proses mengubah teks asli menjadi berbentuk teks yang susah atau bahkan tidak bisa dimengerti[3]. Enkripsi disebut juga dengan proses perubahan plaintext menjadi ciphertext. Proses pengubahan teks ini dilakukan dengan menggunakan rumus-rumus yang sudah ada menurut algoritma masing-masing. Contoh, jika menggunakan algoritma rail fence cipher maka cara mengenkripsi teksnya dengan cara menyusun teks secara diagonal pada baris dan kolom sesuai kunci yang yang dibuat, misalkan dengan kunci dua baris. Maka teks akan disusun secara zig-zag sesuai dengan cara yang digunakan.

## Dekripsi

Teknik dekripsi juga diperlukan dalam sebuah pengamanan teks. Dekripsi adalah proses kebalikan dari enkripsi yaitu mengubah pesan yang sudah terenkripsi menjadi pesan asli. Dekripsi disebut dengan proses pengembalian ciphertext menjadi plaintext[24]. Pada proses dekripsi ini proses pengubahan teks yang susah dibaca menjadi teks yang bisa dibaca lagi dengan cara membuka teks enkripsi dengan kunci yang sudah ditentukan. Contoh, jika yang akan didekripsi menggunakan algoritma rail fence cipher, maka caranya adalah dengan menghitung jumlah karakter ciphertext, selanjutnya dibagi dengan nilai enkripsi. Maka hasilnya sebagai kunci dekripsi, kemudian susun teks secara diagonal atau zig-zag.

## Algoritma Kriptografi

**2.2.7.1. Algoritma Kriptografi Simetris**

Algoritma simetris adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm*. Algoritma enkripsi dekripsi ini memiliki kunci enkripsi sama dengan kunci dekripsi. Pada gambar 2.2 dijelaskan diagram proses enkripsi dan dekripsi algoritma asimetris.

Plaintext Chipertext Plaintext

Dekripsi

Enkripsi

kunci enkripsi kunci dekripsi

### ***Gambar 2.2.*** Diagram proses enkripsi dan dekripsi algoritma simteris

Kelebihan algoritma kriptografi simetris adalah:

1. Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma

asimetrik.

1. Karena kecepatannya yang cukup tinggi, maka dapat digunakan

pada sistem *real-time*

Kekurangan algoritma kriptografi simetris adalah:

1. Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.

Contoh algoritma kriptografi simetris : Rail fence cipher, Rijndael

**2.2.7.2. Algoritma Kriptografi Asimetris**

Algoritma asimetris adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik dan kunci privat. Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan. Pada gambar 2.3 dijelaskan diagram proses enkripsi dan dekripsi algoritma asimetris.

Plaintext Chipertext Plaintext

Dekripsi

Enkripsi

kunci enkripsi (k1) kunci dekripsi (k2)

### ***Gambar 2.3.*** Diagram proses enkripsi dan dekripsi algoritma asimteris

Kelebihan algoritma kriptografi asimetris :

1. Masalah keamanan pada distribusi kunci dapat lebih baik
2. Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit

Kelemahan algoritma kriptografi asimetris:

1. Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris.
2. Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.

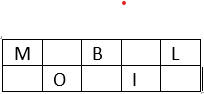
Contoh algoritma : RSA, DSA, ElGamal

## Algoritma Rail Fence Cipher

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 atau teks pada plaintext sehingga didapatkan suatu enkripsi yang berbeda dari pesan aslinya[25]. Algoritma rail fance dikenal juga dengan algoritma zig-zag, karena pada algoritma rail fence teks di susun secara zig-zag. Kunci dari metode ini adalah seberapa banyak baris yang digunakan untuk melakukan proses enkripsi dan deskripsi. Baris yang digunakan harus lebih dari satu baris. Selanjutnya teks dibaca secara baris per baris.

Contoh langkah – langkah yang perlu dilakukan untuk mengenkripsi teks dalam algoritma rail fence cipher adalah sebagai berikut :

1. Teks yang akan dienkripsi adalah MOBIL dengan menggunakan kunci dua baris.
2. Teks ditulis secara berurutan secara diagonal.



### **Gambar 2.4.** Algoritma Rail Fence Cipher

1. Untuk mendapatkan hasil enkripsi, teks ditulis secara berurutan dari kiri ke kanan dimulai dari baris yang paling atas. Sehingga diperoleh ciphertext yaitu MBLOI.

Algoritma rail fence cipher adalah metode yang menggunakan tabel kolom dan baris dalam mengenkripsi sebuah teks, kunci yang dibutuhkan harus lebih dari satu baris.

Berikut ini adalah rumus enkripsi dari metode rail fence cipher :

Ci = Pi(key)....................(1)

Berikut ini adalah rumus dekripsi dari metode rail fence cipher :

Kd = Len(C)/Ke..............(2)

Kunci untuk menggunakan dekripsi yaitu :

Pi = Ci(Kd).....................(3)

Contoh proses enkripsi :

Plaintext : LAPTOPBARU

Kunci : 3 baris

Cara menentukan panjang kolom dengan cara menghitung jumlah karakter pada plaintext.

Baris 2

Baris 1

Baris 3

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L |  |  |  | O |  |  |  | R |  |
|  | A |  | T |  | P |  | A |  | U |
|  |  | P |  |  |  | B |  |  |  |

Ciphertext : LORATPAUPB

Contoh proses dekripsi : (ciphertext ditulis menyamping)

Ciphertext : LORATPAUPB

Kunci : 3 baris

Jumlah karakter : 10 karakter

Karena jumlah plaintext 10 karakter maka kolom yang dibuat adalah sebanyak 10 kolom/kotak.

Baris 2

Baris 3

Baris 1

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L |  |  |  | O |  |  |  | R |  |
|  | A |  | T |  | P |  | A |  | U |
|  |  | P |  |  |  | B |  |  |  |

Plaintext : LAPTOPBARU

## Evaluasi

Berdasarkan permasalahan dalam keamanan dalam pertukaran informasi, proses yang dilakukan oleh metode rail fence cipher adalah dengan melakukan transposisi terhadap informasi berupa teks rahasia[25]. Penggunaan metode algoritma rail fence cipher untuk mengamankan teks pada saat pertukaran informasi bisa dikatakan efektif jika hanya penyandian teks. Namun tidak pada penyandian gambar, video, dan pesan suara. Dikarenakan peneliti hanya menguji dengan menggunakan objek teks saja. Metode ini memiliki kelemahan dimana abjad dalam ciphertext terdiri dari abjad teks biasa.

## Kerangka Pemikiran

**Rumusan Masalah**

Bagaimana mengamankan pertukaran informasi berbasis teks memanfaatkan teknik kriptografi

**Pendekatan**

Menggunakan metode algoritma kriptografi rail fence cipher

**Penerapan**

Algoritma rail fence cipher diterapkan pada sebuah aplikasi

**Tujuan**

Menerapkan metode rail fence cipher untuk mengamankan pertukaran informasi berbasis teks

**Hasil**

Hasil berupa alat simulasi enkripsi dan dekripsi untuk penyandian informasi berbasis teks

# BAB III

# METODOLOGI PENELITIAN

## Gambaran Umum Penerapan Algoritma

Penerapan metode yang digunakan adalah metode algoritma rail fence cipher yang dapat mengenkripsi teks yang semula bisa dibaca menjadi teks yang susah dibaca. Metode ini diterapkan pada sebuah aplikasi kriptografi yang dapat mengenkripsi sebuah pesan dan meneruskan hasilnya sebagai teks pesan ke aplikasi pengiriman pesan seperti aplikasi SMS, Whatsapp, Line, dan sejenisnya.

## Flowchart Enkripsi

*Flowchart* sistem mennggambarkan urutan proses secara mendetail dan

hubungan antara satu proses dengan proses lainnya. *Flowchart* sistem untuk enkripsi data dapat dilihat pada Gambar 3.1.

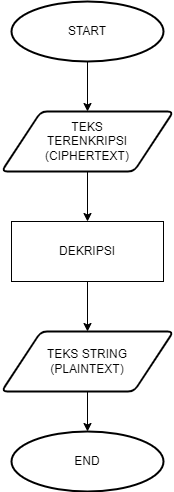


### ***Gambar 3.1.*** *Flowchart* enkripsi teks

Berdasarkan gambar 3.1, Penjabaran dari *flowchart* enkripsi adalah teks string sebagai plaintext berupa teks biasa yang terdiri dari abjad A-Z. Proses enkripsinya adalah teks string dienkripsi dengan cara mengubah teks biasa yang semulanya bisa dibaca menjadi teks yang tidak bisa dibaca dan dimengerti menggunakan algoritma rail fence cipher sehingga keluaran dari teks yang terenkripsi menjadi ciphertext.

## Flowchart Dekripsi

*Flowchart* untuk dekripsi dapat dilihat pada gambar 3.2.



### ***Gambar 3.2.*** *Flowchart* dekripsi teks

Berdasarkan Gambar 3.2, Penjabaran dari *flowchart* dekripsi adalah teks yang terenkripsi (ciphertext) akan didekripsi menggunakan proses metode algoritma rail fence cipher, yang mana ciphertext akan dirubah menjadi plaintext kembali. Hasil keluaran dari dekripsi merupakan teks yang bisa dibaca secara normal.

## Pengujian Penerapan Algoritma

Teknik pengujian dilakukan dengan menggunakan *whitebox* dan menggunakan teks kata dan kalimat yang berbeda-beda. Dan dilakukan untuk proses enkripsi dan dekripsi teks, dimana aplikasi yang digunakan untuk menguji penerapan algoritma ini adalah berbasis web.

# DAFTAR PUSTAKA

[1] A. Hermawan and H. I. E. Ujianto, “InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA,” *J. Nas. Inform. dan Teknol.*, vol. 2, no. 1, 2021.

[2] M. Azwar, M. Qulub, and F. Fatimatuzzahra, “Kombinasi Metode Kriptografi Subsitusi Dalam Pengaman Pesan dan Informasi,” *ICIT J.*, vol. 8, no. 2, pp. 172–180, 2022, doi: 10.33050/icit.v8i2.2407.

[3] Imam Riadi, Abdul Fadlil, and Fahmi Auliya Tsani, “Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher,” *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 33–45, 2022, doi: 10.14421/jiska.2022.7.1.33-45.

[4] E. Yoppi and Z. Situmorang, “Aplikasi Tanda Tangan Digital Dengan Algoritma Gost Untuk Keamanan Pengiriman File Dokumen,” *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 03, no. 01, pp. 13–21, 2021, [Online]. Available: http://dx.doi.org/10.54367/kakifikom.v3i1.1196%0Ahttp://ejournal.ust.ac.id/index.php/KAKIFIKOM/article/download/1196/pdf1.

[5] L. D. Simatupang and U. D. Bengkulu, “Pengamanan Dokumen Teks Dengan Menerapkan Kombinasi Algoritma Kriptografi Klasik,” vol. 07, pp. 133–140, 2022.

[6] F. Efendi, J. Informatika, U. A. Yogyakarta, and C. Catur, “Implementasi Kriptografi dalam Sistem Keamanan Anjungan Tunai Mandiri,” vol. 5, no. 1, pp. 51–54, 2019.

[7] W. P. Abdul Kodir, “IMPLEMENTASI KRIPTOGRAFI DENGAN MENGGUNAKAN METODE RC4 DAN BASE64 UNTUK MENGAMANKAN DATABASE SEKOLAH PADA SDN GROGOL UTARA 10,” vol. 4, no. 1, pp. 7–14, 2021.

[8] E. Dokumen, G. Geulis, and E. Abadi, “Penerapan Algoritma AES ( Advance Encryption Standart ) 128 untuk,” vol. 5, pp. 1–10, 2022.

[9] T. Lovian and I. Fitri, “Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang,” vol. 6, pp. 692–700, 2022, doi: 10.30865/mib.v6i1.3513.

[10] A. Masduki and I. K. G. Suhartana, “Proteksi Aplikasi Pesan SMS Berbasis Mobile Android Dengan Algoritma AES 256 dan Steganografi LSB,” vol. 7, no. 3, pp. 203–209, 2019.

[11] D. Ratna, “Implementasi Algoritma Rail Fence Chiper dalam Keamanan Data Gambar 2 Dimensi,” *Pelita Inform. Inf. dan …*, vol. 7, pp. 38–42, 2018.

[12] M. H. Jannah and H. Aspriyono, “Implementasi Algoritma Caesar Chiper dan Rail Fence untuk Peningkatan Keamanan Teks Berbasis Client Server Coding & Testing Penerapan Pemeliharaan,” vol. 6, no. 2, 2021.

[13] A. P. Simamora *et al.*, “Perancangan Aplikasi Keamanan File PDF Dengan Algoritma Rail Fence + Xor Berbasis Android,” pp. 57–70.

[14] M. Fadlan, S. Sinawati, A. Indriani, and E. D. Bintari, “Pengamanan Data Teks Melalui Perpaduan Algoritma Beaufort Dan Caesar Cipher,” *J. Tek. Inform.*, vol. 12, no. 2, pp. 149–158, 2019, doi: 10.15408/jti.v12i2.12262.

[15] Sinawati, Indrianti, and M. Hafid, “Analisa Kriptografi Block Cipher pada Pengamanan Teks Menggunakan Metode Triple Transposition Vigenere Cipher,” *Pros. SNATIF ke-6 Tahun 2019*, no. 2007, pp. 96–101, 2019.

[16] P. Kriptografi and C. Chiper, “APLIKASI CHATTING BERBASIS LOCAL AREA NETWORK,” vol. 4, no. 1, pp. 1–10, 2021.

[17] M. Sari, H. D. Purnomo, and I. Sembiring, “Review : Algoritma Kriptografi Sistem Keamanan SMS di Android,” *J. Inf. Technol.*, vol. 2, no. 1, pp. 11–15, 2022, doi: 10.46229/jifotech.v2i1.292.

[18] Istiqomah, “Exact Papers in Compilation,” *Exact Pap. Compil.*, vol. 2, no. 1, pp. 211–218, 2020.

[19] D. Syariati, U. Ludigdo, and A. Djamhuri, “Jurnal Akuntansi Aktual,” *J. Akunt. Aktual*, vol. 7, no. 2004, pp. 57–66, 2020.

[20] P. T. B. J. Mandiri, U. Padjadjaran, and U. Padjadjaran, “Pertukaran Informasi Oleh Mahasiswa Jurusan Ilmu,” vol. 3, no. 1, pp. 71–80, 2015.

[21] E. M. Safitri, Z. Ameilindra, and R. Yulianti, “Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur,” *J. Ilm. Teknol. Inf. dan Robot.*, vol. 2, pp. 21–26, 2020.

[22] E. P. Rahayu and H. Zakaria, “Analisis Keamanan Jaringan Komputer Menggunakan Sistem Firewall Untuk Mencegah Serangan Jaringan Internet Dengan Metode …,” *… Semin. Inform. Dan …*, vol. 6, pp. 155–160, 2022.

[23] T. S. Alasi, R. Wanto, and V. H. Sitanggang, “Implementasi Kriptografi Algoritma Idea Pada Keamanan Data Teks Berbasis Android,” *J. Inf. Komput. Log.*, vol. 2, no. 1, pp. 1–4, 2021.

[24] M. Ziaurrahman, E. Utami, and F. W. Wibowo, “Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut,” *J. Inform. dan Teknol. Inf.*, vol. 4, no. 1, pp. 63–68, 2019.

[25] D. Elgamal *et al.*, “Aplikasi Pengamanan File Gambar Menggunakan Rail Fence Cipher Dan Image File Security Application Using Rail Fence Cipher,” vol. 8, no. 2, pp. 132–140, 2020.