

## Implementasi Algoritma Caesar Chiper dan Rail Fence untuk Peningkatan Keamanan Teks Berbasis Client Server

<sup>1)</sup> Mifta Halul Jannah

Univesitas Dehasen, Jl.Merpati Raya No.32 Telp. (0735) 22027, Kota Bengkulu, Indonesia  
E-Mail: [haluljannahmifta@gmail.com](mailto:haluljannahmifta@gmail.com)

<sup>2)</sup> Khairil

Univesitas Dehasen, Jl.Merpati Raya No.32 Telp. (0735) 22027, Kota Bengkulu, Indonesia  
E-Mail: [khairil@unived.ac.id](mailto:khairil@unived.ac.id)

<sup>3)</sup> Hari Aspriyono

Univesitas Dehasen, Jl.Merpati Raya No.32 Telp. (0735) 22027, Kota Bengkulu, Indonesia  
E-Mail: [hari.aspriyono@gmail.com](mailto:hari.aspriyono@gmail.com)

### ABSTRACT

SMK Negeri 3 Bengkulu City is one of the vocational schools in Bengkulu City. The school has a major in Computer and Network Engineering (TKJ). Students will be taught about basic knowledge in computers, network infrastructure, network security and others. Cryptography is part of a security system, where cryptography is the science and art of keeping messages secure. Increased security in the form of an encryption process that is carried out through 2 stages before getting the encryption results, namely encryption using the Caesar Cipher Algorithm and then being encrypted again using the Rail Fence Algorithm. To assist the text security system at SMK Negeri 3 Bengkulu City, a client server-based application was built using the Visual Basic .Net programming language with SQL Server database. In its application, one laptop will be used as a database server, so that the results of inputting text that will be sent to the recipient are automatically stored on the server. While the client only accesses the form of sending and receiving messages through the application that has been provided. If you enter an incorrect or incorrect key, then the plaintext cannot be changed to its original form so that the text message cannot be read.

**Keyword :** implementasi, algoritma caesar chiper, algoritma rail fence chiper, keamanan teks, client server

### PENDAHULUAN

Dunia teknologi informasi sekarang ini berkembang sangat pesat dan mempengaruhi hampir seluruh aspek kehidupan manusia. Perkembangan tersebut secara langsung maupun tidak langsung mempengaruhi semua sistem yang berhubungan ataupun tidak dengan sistem informasi itu sendiri seperti perdagangan, transaksi, bisnis, perbankan, industri dan pemerintahan. Dengan perkembangan teknologi saat ini, setiap orang akan mudah memperoleh data atau informasi

Keamanan dan kerahasiaan data atau informasi merupakan salah satu aspek yang penting dari suatu data atau informasi. Masalah keamanan dan kerahasiaan data komputer merupakan sesuatu yang penting dalam era informasi ini terutama bagi suatu organisasi atau perusahaan. Berbagai cara pun dilakukan untuk melindungi data atau informasi tersebut.

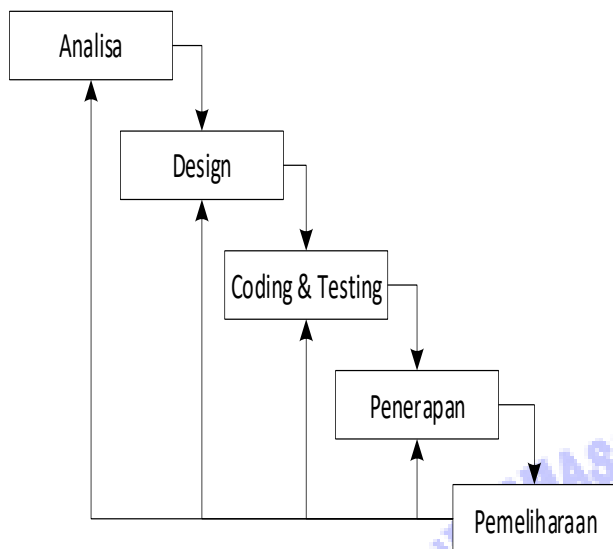
SMK Negeri 3 Kota Bengkulu merupakan salah satu sekolah kejuruan yang terdapat di Kota Bengkulu. Pada sekolah tersebut memiliki jurusan Teknik Komputer dan Jaringan (TKJ). Siswa/i akan diajarkan tentang pengetahuan dasar dalam

komputer, infrastruktur jaringan, keamanan jaringan dan lain-lain. Kriptografi merupakan bagian dari sistem keamanan, dimana kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan.

Kriptografi diklasifikasikan menjadi 2 (dua) bagian yaitu kriptografi klasik dan kriptografi modern. Pada penelitian ini menggunakan kriptografi klasik menggunakan algoritma *caesar chiper* (metode substitusi) dan *rail fence* (metode transposisi). Dalam proses keamanan teks pesan terdapat 2 bagian yaitu proses enkripsi dan proses dekripsi. Enkripsi digunakan untuk mengubah teks asli ke teks yang tidak dapat dibaca melalui tahapan pertama algoritma *chiper*, hasil enkripsi dari algoritma *caesar chiper* tersebut di enkripsi lagi melalui tahapan kedua algoritma *rail fence*. Dekripsi digunakan untuk mengubah teks yang tidak dapat dibaca ke teks asli melalui tahapan pertama algoritma *rail fence*, hasil dekripsi dari algoritma *rail fence* tersebut di dekripsi lagi melalui tahapan kedua algoritma Caesar Chiper.

## METODE PENELITIAN

Metode penelitian yang diterapkan pada penelitian ini adalah dengan pengembangan metode waterfall. Metode Waterfall memiliki tahapan-tahapan terlihat pada Gambar 1.



Gambar 1. Tahapan Metode Waterfall

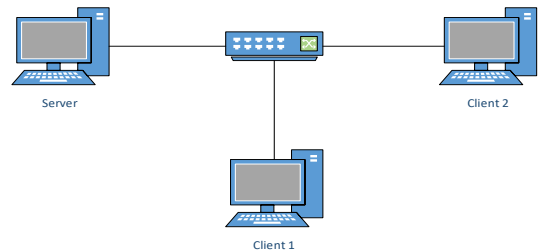
Pada tahap (1) Analisa dilakukan analisis terhadap algoritma kriptografi dalam mengamankan teks. (2) Design dilakukan perancangan sistem berdasarkan hasil analisis. Tahap ini akan menggambarkan rancangan proses penerapan algoritma kriptografi dalam mengamankan data. (3) Coding dan Testing merupakan proses pembuatan aplikasi serta uji coba aplikasi, dimana pada aplikasi tersebut sudah diintegrasikan algoritma kriptografi untuk proses enkripsi dan dekripsi. (4) dilakukan penerapan dari aplikasi yang telah dibuat dengan menguji coba aplikasi. (5) Pemeliharaan dilakukan secara berkala dari aplikasi, jika suatu saat terjadinya eror.

## HASIL DAN PEMBAHASAN

Implementasi Algoritma Caesar Chiper dan Rail Fence untuk peningkatan keamanan teks berbasis client server di SMK Negeri 3 Kota Bengkulu. Peningkatan keamanan berupa proses enkripsi yang dilakukan melalui 2 tahapan sebelum mendapatkan hasil enkripsi yaitu enkripsi menggunakan Algoritma Caesar Chiper kemudian dienkripsi lagi menggunakan Algoritma Rail Fence. Untuk membantu sistem keamanan teks di SMK Negeri 3 Kota Bengkulu ini, maka dibangun aplikasi berbasis client server menggunakan bahasa Pemrograman Visual Basic .Net dengan database SQL Server. Dalam penerapannya 1 laptop akan dijadikan database server, sehingga hasil penginputan teks yang akan dikirim ke penerima secara otomatis tersimpan di server. Sedangkan client hanya mengakses form pengiriman dan penerima pesan melalui aplikasi yang telah

disediakan.

Adapun skema jaringan yang sudah dibangun melalui uji coba 3 laptop seperti Gambar 2.



Gambar 2. Skema Jaringan

Pada Gambar 2 terlihat bahwa terdapat 2 PC yang terhubung melalui hub, di mana masing-masing PC telah diberikan IP Address masing-masing. Adapun menu antarmuka pada sistem keamanan teks di SMK Negeri 3 Kota Bengkulu berbasis client server, antara lain: **Form Login** merupakan form yang digunakan untuk membatasi hak akses penggunaan aplikasi. Bagi user yang belum memiliki akun untuk masuk ke aplikasi, maka klik tombol daftar, dan bagi user yang sudah memiliki akun untuk masuk ke aplikasi klik tombol login seperti Gambar 3.

Gambar 3. Form Login

**Menu Utama** merupakan antarmuka aplikasi yang muncul ketika user berhasil melakukan login. Pada menu utama terdapat form yang dapat diakses yaitu form pengiriman pesan dan form penerima pesan. Adapun antarmuka menu utama seperti Gambar 4.



Gambar 4. Menu Utama

**Form Update Kunci** merupakan form yang digunakan untuk mengubah kunci yang digunakan dalam proses enkripsi dan dekripsi pesan yang dikirim atau diterima. Yang dapat mengupdate kunci adalah admin. Adapun form update kunci, seperti Gambar 5.

Gambar 5. Form Update Kunci

**Form Pengiriman Pesan** merupakan form yang digunakan untuk membantu user dalam mengirimkan pesan ke user penerima dengan cara mengetik pesan kemudian memasukkan kunci caesar chiper dan kunci rail fence chiper, pesan yang dikirim adalah yaitu pesan yang telah terenkripsi dan tersimpan ke dalam database server. Adapun form pengiriman pesan seperti Gambar 6.

Gambar 6. Form Pengiriman Pesan

**Form Penerima Pesan** merupakan form yang digunakan untuk membantu user melihat pesan yang diterima/pesan yang dikirim oleh pengirim. untuk membuka pesan tersebut, penerima harus memasukkan kunci yang sama sesuai ketentuan antara pengirim dan penerima. Adapun form penerima pesan seperti Gambar 7.

Gambar 7. Form Penerima Pesan

**Keluar** digunakan untuk keluar dari aplikasi jika sudah selesai menggunakan aplikasi ini.

## KESIMPULAN

Berdasarkan hasil penelitian dapat disimpulkan bahwa: (1.)Peningkatan keamanan berupa proses enkripsi yang dilakukan melalui 2 tahapan sebelum mendapatkan hasil enkripsi yaitu enkripsi menggunakan Algoritma Caesar Chiper kemudian dienkripsi lagi menggunakan Algoritma Rail Fence. (2.) Untuk membantu sistem keamanan teks di SMK Negeri 3 Kota Bengkulu ini, maka dibangun aplikasi berbasis client server menggunakan bahasa Pemrograman Visual Basic .Net dengan database SQL Server. (3.) Dalam penerapannya 1 laptop akan dijadikan database server, sehingga hasil penginputan teks yang akan dikirim ke penerima secara otomatis tersimpan di server. Sedangkan client hanya mengakses form pengiriman dan penerima pesan melalui aplikasi yang telah disediakan. (4.) Jika memasukkan kunci yang tidak sesuai atau salah, maka plaintext tidak dapat berubah ke bentuk semula sehingga pesan teks tidak dapat dibaca.

## SARAN

Berdasarkan kesimpulan, maka penulis menyarankan agar dapat menggunakan aplikasi ini untuk mengamankan pesan yang akan dikirim ke komputer lain.

## DAFTAR PUSTAKA

- [1] Blazing, A., 2018. Pemrograman Windows Dengan Visual Basic .Net : Praktikum Pemrograman VB.Net. s.l.:Google Book.
- [2] Indrajani., 2017. Database Design Theory, Practice, and Case Study. Jakarta: PT. Elex Media Komputindo.
- [3] Jamaludin & Romindo, 2020. Kriptografi : Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vigenere Cipher dan RSA. Medan: Yayasan Kita Menulis.
- [4] Khasanah, F. N., 2016. Perancangan dan Simulasi Jaringan Komputer Menggunakan Graphical Network Simulator 3 (GNS3). Makalah Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta..
- [5] Kusumo, A. S., 2016. Administrasi SQL Server 2014. Jakarta: PT. Elex Media Komputindo.
- [6] Latifah, R., Ambo, S. N. & Kurnia, S. I., 2017. Modifikasi Algoritma Caesar Chiper dan Rail Fence Untuk Peningkatan Keamanan Teks Alfanumerik dan Karakter Khusus. Jakarta, Seminar Nasional Sains dan Teknologi Fakultas Teknik Universitas Muhammadiyah Jakarta.
- [7] Mukhtar, H., 2018. Kriptografi Untuk Keamanan Data. Yogyakarta: Deepublish.

- [8] Purba, D. F. & Puspasari, R., 2020. Penerapan Algoritma Rail Fence Untuk Penghasil Pesan Rahasia Berbasis Android. Jurnal FTIK, Volume Vol.1 No.1.
- [9] Ratna, D., 2018. Implementasi Aglrotima Rail Fence Chiper Dalam Keamanan Data Gambar 2 Dimensi. Jurnal Pelita Informatika , Volume Vol.17. No. 3. ISSN : 2301-9425.
- [10] Rusmala & Prasti, D., 2019. Implementasi Metode Rail Fence Chiper dan Row Transposition Chiper Pada Mata Kuliah Kriptografi. Jurnal Ilmiah d'Computare , Volume Vol.9.
- [11] Santoso & Nurmalina, R., 2017. Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut). Jurnal Integrasi , Volume Vol.9 No.1 . E-ISSN : 2548-9828.
- [12] Siahaan, V. & Sianipar, R. H., 2019. Database Dan Kriptografi Menggunakan Java/MySQL. Yogyakarta: Sparta Publishing.
- [13] Sutoyo, M. N. & Murhaban, 2016. Kombinasi Algoritma Kriptografi Caesar Chiper dan Vigenere Chiper Untuk Keamanan Data. Jurnal Mekanova, Volume Vol.2 No.1 ISSN 2502-0498.
- [14] Wicaksono, S. R., 2019. Jaringan Komputer Konsep dan Studi Kasus. Pertama penyunt. Malang Jawa Timur: CV. Seribu Bintang.
- [15] Yudiantoro, D. C., 2020. Modifikasi Metode Kriptografi Caesar Cipher Menggunakan Deret Simbol Pada Keyboard Smartphone. Jurnal Teknologi Informasi, Volume Vol.4 No.2 p-ISSN.2580-7927.