IMPLEMENTASI KRIPTOGRAFI BERBASIS CAESAR CHIPER UNTUK KEAMANAN DATA

Rindy Febrianingsih[1] Aliy Hafiz[2]
Manajemen Informatikan, AMIK Dian Cipta Cendikia[12]
Jl. Cut Nyak Dien No. 65 Durian Payung (Palapa) Bandar Lampung
E-mail : rindy234@gmail.com[1] , hafizdahsyat@gmail.com[2]

Abstrak

Kriptografi merupakan bagian ilmu yang mempelajari tentang cara menjaga agar data atau pesan tetap aman. algoritma kriptografi teknis terdiri dari substitusi dan transposisi pada data. teknik kriptografi dapat digunakan untuk menangani masalah kebocoran pada data atau informasi, karena kriptografi menggunakan rumus-rumus matematika, mulai dari rumus sederhana sampai kepada rumus yang kompleks. Pada penelitian ini digunakan algoritma caesar chiper. Algoritma caesar cipher termasuk pada kriptografi klasik yang memiliki kunci simestris. Dari hasil penelitian ini dapat disimpulkan bahwasanya algoritma caesar chiper dapat membantu dalam mengamankan data sehingga kebocoran data bisa diminimalisir.

Kata kunci **:** kriptografi, caesar, chiper, keamanan, data

Abstract

Cryptography is a part of science that studies about how to keep data or messages safe. Technical cryptographic algorithms consist of substitution and transposition of data. cryptographic techniques can be used to deal with leakage problems in data or information, because cryptography uses mathematical formulas, ranging from simple formulas to complex formulas. In this study caesarean cipher algorithm was used. Caesarean cipher algorithm is included in classical cryptography which has a symmetrical key. From the results of this study it can be concluded that the caesarean cipher algorithm can help in securing data so that data leakage can be minimized.

Keywords: cryptography, caesar, cipher, security, data

1. PENDAHULUAN

Keamanan menjadi aspek yang sangat penting saat ini di mana pertukaran data dan informasi menjadi tuntutan baik pekerjaan dan lainnya. Berbagai cara dilakukan untuk mengamankan data atau informasi di antaranya menggunakan Kriptologi. Kriptografi merupakan bagian ilmu yang mempelajari tentang cara menjaga agar data atau pesan tetap aman. Beragam macam teknik digunakan untuk upaya mengamankan data atau informasi yang penting [1].

Pada pengamanan dalam kriptografi ini banyak metode atau algoritma yang dapat digunakan, seperti Caesar, Abjad Majemuk, DES, IDEA, RSA dan lain sebagainya. Sedangkan pada penelitian ini menggunakan metode Caesar Chiper. Algoritma caesar cipher termasuk pada kriptografi klasik yang memiliki kunci simestris (hanya ada satu kunci) yang mana biasa digunakan dalam mengekripsi ataupun mendekripsi data dan informasi. Karena caesar chiper merupakan kriptografi klasik maka proses enkripsi dan dekripsinya dilakukan dengan cara substitusi atau perpindahan.

Kriptografi merupakan dasar untuk memahami keamanan pada komputer. Caesar Chiper merupakan sistem persandian berbasis substitusi. Adapun dalam proses Enskripsi dan deskripsi pada metode Caesar menggunakan operasi shift. Cara kerja operasi shift adalah dengan cara mensubstitusikan huruf-huruf pada alfabet yang berada di sebelah kiri atau sebelah kanan huruf tersebut. Sedangkan chiper alphabet majemuk adalah chiper substitusi ganda yang melibatkan penggunaan kunci berbeda atau huruf kapital dan lainnya [2].

Begitu pentingnya kriptografi untuk keamanan informasi, sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkannya dengan kriptografi. Maka dari

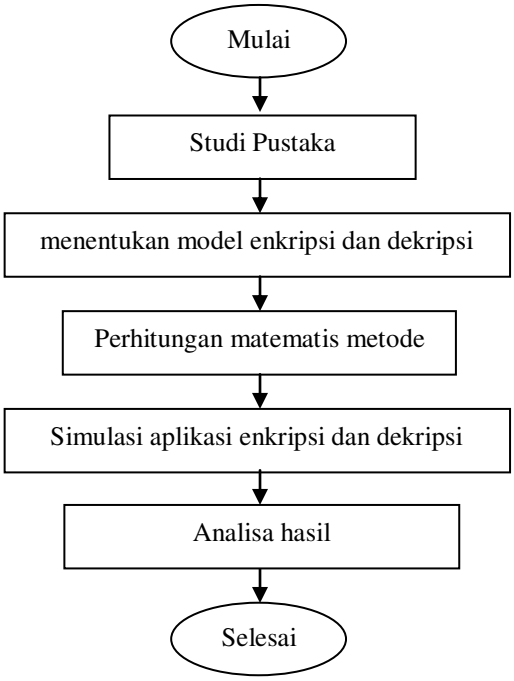
itu upaya yang dilakukan untuk melakukan pengamanan data tersebut yaitu dengan melakukan enkripsi.

2. METODE PENELITIAN

2.1 Jenis Penelitian

Jenis penelitian yang dilakukan adalah penelitian terapan, yaitu penelitian yang bertujuan untuk menyelesaikan masalah yang ada dengan menerapkan teori-teori yang mendasari penelitian yang dikaji dengan terlebih dahulu menyusun konsep-konsep yang berkaitan dengan kriptografi secara matematis, dengan DELPHI sebagai alat bantu komputasi[3].

Pada bagian ini dijelaskan mengenai metode yang digunakan dalam penelitian ini. Metode penelitian ini meliputi penentuan model enkripsi, penyelesaian algoritma enkripsi, pembuatan simulasi enkripsi dan analisa hasil dari simulasi enkripsi [4]. Diagram alir perancangan simulasi pada penelitian ini secara lengkap dapat dilihat pada Gambar 1 di bawah ini.



Gambar 1 diagram alir simulasi enkripsi dan dekripsi

Pada gambar 1 di atas dapat diketahui penelitian ini dimulai dari studi pustaka, setelah menemukan permasalahan kemudian menentukan model enkripsi dan dekripsi, langkah selanjutnya adalah menentukan perhitungan matematis. Setelah menentukan perhitungan matematis dibuat aplikasi simulasi sebagai uji coba dari perhitungan matematis tersebut dan di analisa apakah sudah benar atau belum.

2.2 Metode pengembangan sistem

Metode pengembangan sistem yang penulis gunakan dalam penelitian ini adalah metode *Extreme Programming*. *Extreme Programming* yaitu sebuah metode dalam pengembangan sistem yang dilakukan untuk membuat pembaruan sistem yang berjalan[5]. Berikut ini adalah tahapan-tahapan yang akan dilakukan dengan menggunakan metode *Extream Programming* :

1. *Planning*/Perencanaan

Pada tahap perencanaan ini dimulai dari pengumpulan kebutuhan yang membantu tim teknikal untuk memahami konteks bisnis dari sebuah aplikasi. Selain itu pada tahap ini juga mendefinisikan output yang akan dihasilkan, fitur yang dimiliki oleh aplikasi dan fungsi dari aplikasi yang dikembangkan.

2. *Design*/Perancangan

Metode ini menekankan desain aplikasi yang sederhana, bagaimana sebuah aplikasi bisa berjalan dengan baik.

3. *Coding*/Pengkodean

Konsep utama dari tahapan pengkodean pada *extreme programming* adalah bagaimana menyusun kode yang sederhana sehingga mudah dipahami.

4. *Testing*/Pengujian

Pada tahapan ini lebih fokus pada pengujian fitur dan fungsionalitas dari aplikasi.

2.3 Borland Delphi

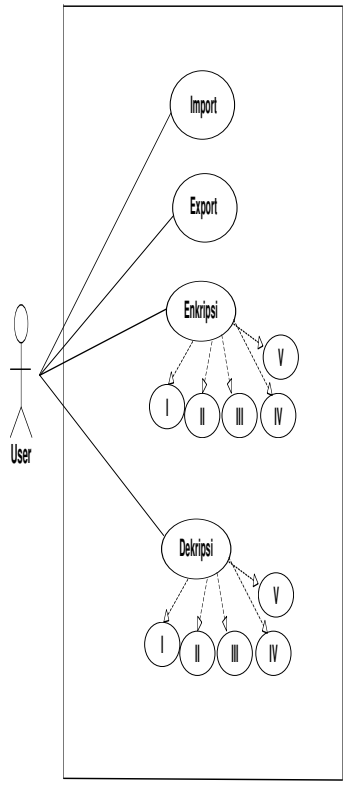
Borland Delphi pada awalnya adalah proyek rahasia yang berevolusi menjadi produk yang disebut dengan App Builder. Namun sebelum rilis pertama dari borland delphi, novell yang menjadi app builder sudah dirilis sehingga borland harus memberikan nama baru untuk proyek tersebut. Adapun tujuan dari delphi pada waktu itu adalah menyediakan konektivitas database untuk programmer yang akan menjadi fitur kunci pada database karena pada waktu itu yang paling populer adalah database oracle[6].

2.4 Perancangan Sistem

Tahap perancangan sistem adalah setelah tahap analisa sistem selesai dilakukan, maka analisa sistem mendapatkan gambaran dengan jelas tentang apa yang harus dilakukan, selanjutnya analisa sistem memikirkan bagaimana membentuk sistem tersebut. Adapun alat rancang yang digunakan adalah sebagai berikut:

a. Usecase

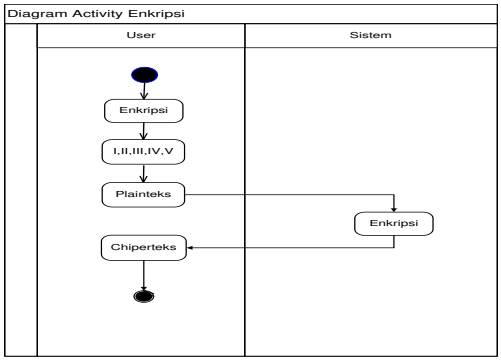
Diagram *Use Case* merupakan bagian tertinggi dari fungsionalitas yang dimiliki sistem yang akan menggambarkan bagaimana seseorang atau actor akan menggunakan dan memanfaatkan sistem. Diagram ini juga mendeskripsikan apa yang akan dilakukan oleh sistem. Diagram *use case* pusat peminjaman ruangan dan peralatan dapat dilihat pada gambar dibawah ini:



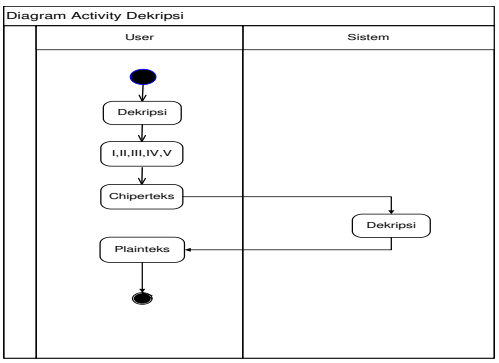
Gambar 2 Usecase sistem enkripsi dan dekripsi

b. Activity Diagram

Activity Diagram memberikan gambaran rancangan alur disetiap fungsi yang ada di dalam system. *Activity diagram* menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir.



Gambar 3 Diagram activity enkripsi



Gambar 4 Diagram activity enkripsi

Pada gambar 5 di atas dapat dilihat panel kiri atas merupakan pilihan antara enkripsi atau dekripsi, kemudian di sampingnya ada pilihan untuk melakukan pergeseran antara 1 sampai 5 pergeseran, dan di bawah panel itu adalah input untuk plainteks yaitu teks yang akan di enkripsi, kemudian di bawah panel itu ada chiper text yaitu hasil dari proses enkripsi. Pada panel sebelah kanan merupakan fitur untuk import dan export, yaitu fitur untuk mengambil file yang ada di dalam komputer kemudian export untuk menyimpan hasil enkripsi ke dalam komputer dalam bentuk file teks yang bisa dibuka dengan notepad.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Perhitungan Matematis

Data yang digunakan untuk pesan *(plaintext)* yaitu berupa karakter dalam bentuk karakter huruf a-z, angka 1-9, dan tanda baca seperti koma(,), titik (␣), tanda tanya (?), tanda seru (!)

dan lainnya, tetapi pada penelitian ini hanya dilakukan enkripsi dan dekripsi pada karakter huruf saja, di mana pesan tersebut akan dilakukan proses enkripsi menggunakan metode kriptografi *caesar chiper*, kemudian setelah di enkripsi akan menghasilkan *ciphertext*. *Ciphertext* ini kemudian bisa di dekripsi agar bisa dibaca kembali atau *plaintext*. Tabel substitusi dari perubahan metode caesar adalah sebagai berikut.

Tabel 1 tabel *caesar chiper*

a	b	c	d	e	f	g	h	i	j	k	l	m
n	o	p	q	r	s	t	u	v	w	x	y	z

Pada tabel 1 yang merupakan tabel sumber untuk dijadikan rujukan dalam proses enkripsi, dengan pergeseran 4 karakter. maka jika dilakukan proses enkripsi adalah sebagai berikut:

Plainteks : saya kuliah di dcc
Kunci : bergeser 4 hurup
Chiperteks : wece oypmel hm hgg

Proses enkripsi pada kalimat "saya kuliah di dcc" adalah sebagai berikut:

Tabel 2 substitusi *caesar chiper* bergeser 4 huruf.

Huruf	Substitusi 4
s	w
a	e
y	c
a	e
k	o
u	y
l	p
i	m
a	e
h	l
d	h
i	m
d	h
c	g
c	g

Adapun jika ingin substitusi dengan pergeseran sebanyak 5 huruf maka jika dilakukan proses enkripsi adalah sebagai berikut:

Plainteks : saya kuliah di dcc
Kunci : bergeser 5 huruf
Chiperteks : xfdf pzqnfm in ihh

Proses enkripsi pada kalimat "saya kuliah di dcc" adalah sebagai berikut:

Tabel 3 substitusi *caesar chiper* bergeser 5 huruf.

Huruf	Substitusi 5
s	x
a	f
y	d
a	f
k	p
u	z
l	q
i	n
a	f
h	j
d	i
i	n
d	i
c	h
c	h

3.2 Simulasi Aplikasi Enkripsi

Sistem enkripsi yang peneliti buat ini diharapkan dapat mengamankan data rekam medis pasien sehingga privasi pasien terjaga dan aman. Berikut penjelasan program dari sistem yang siap untuk digunakan :

a. Menu Utama

Menu Utama merupakan halaman utama yang terdiri dari menu enkripsi, dekripsi, pilihan substitusi pergeseran, plainteks, chiperteks, import, clear, export dan keluar. Menu Utama dapat dilihat pada gambar berikut ini:

Gambar 6 menu utama aplikasi enkripsi

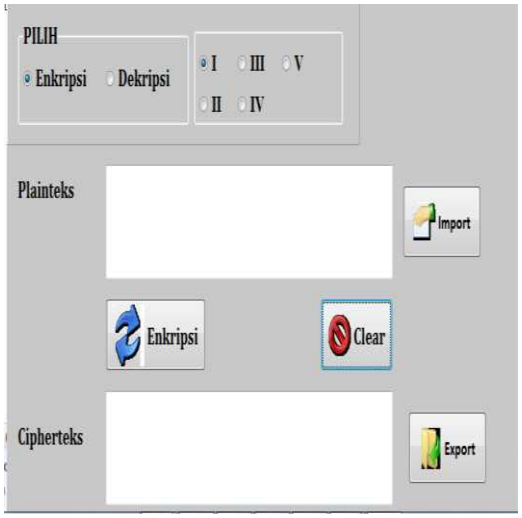
b. Menu Enkripsi

Menu enkripsi adalah menu untuk proses enkripsi file. Menu enripsi bisa dilihat pada gambar berikut ini:

Gambar 7 menu enkripsi

c. Menu Dekripsi

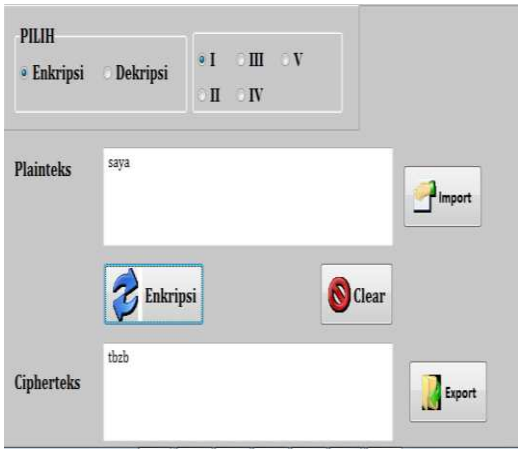
Menu enkripsi adalah menu untuk proses dekripsi file. Menu dekripsi bisa dilihat pada gambar berikut ini:



Gambar 8 menu dekripsi

d. Enkripsi Substitusi 1

Berikut ini adalah hasil enkripsi dengan substitusi pergeseran 1 kali dari huruf. Yaitu dengan bergeser huruf tertentu ke huruf depannya sebanyak 1 kali. Hasil nya adalah:



Gambar 9 hasil substitusi 1 kali

e. Enkripsi Substitusi 2

Berikut ini adalah hasil enkripsi dengan substitusi pergeseran 2 kali dari huruf. Yaitu dengan bergeser huruf tertentu ke huruf depannya sebanyak 2 kali. Hasil nya adalah:

Gambar 10 hasil substitusi 2 kali

4. KESIMPULAN

Berdasarkan hasil dari aplikasi enkripsi menggunakan caesar chiper maka dapat diambil kesimpulan bahwasanya perhitungan matematis caesar chiper bisa dilakukan dengan sistem substitusi satu (1), dua (2), tiga (3), empat (4),

lima (5) dan seterusnya dan aplikasi enkripsi menggunakan caesar chiper yang dapat mengacak file sehingga tidak bisa dibaca membuat data menjadi lebih aman.

DAFTAR PUSTAKA

[1] Apreja, A., Syarif, Z., & Ibrahim, A. (2017, November). Analisis Tingkat Keamanan Enkripsi Data Menggunakan Algoritma Base 64 Endcode. In *Annual Research Seminar (ARS)* (Vol. 3, No. 1, pp. 49-50).

[2] Susanto, S., & Trisusilo, A. A. (2018). Penerapan Algoritma Asimetris Rsa Untuk Keamanan Data Pada Aplikasi Penjualan Cv. Sinergi Computer Lubuklinggau Berbasis Web. *Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, *9*(2), 1043-1052.

[3] Hafiz, A. (2019). Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB). *Jurnal Cendikia*, *17*(1 April), 194-198. (LSB). *Jurnal Cendikia*, *17*(1 April), 194-198.

[4] Lubis, B. O., & Salim, A. (2018, December). Aplikasi Penentuan Mustahik Menggunakan Global Extreme Programming (Studi Kasus: Badan Amil Zakat dan Sedekah Dewan Kemakmuran Masjid Jakarta). In *Seminar Nasional Industri dan Teknologi* (pp. 247-258).

[5] Suliyanto, S. E., & MM, S. (2017). Metode Penelitian Kuantitatif.

[6] Kusnassriyanto, 2011. Belajar Pemrograman Delphi. Bandung. Modula.