APLIKASI CHATTING BERBASIS WEB DENGAN ALGORITMA *CAESAR CIPHER* DAN 3DES PADA CV. FELITECHNO MANDIRI UNTUK PENGAMANAN PESAN PADA DATABASE

Dwika Arief Prasada[1)], **Purwanto**[2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
E-mail : mail.dwikaarief@gmail.com[1)], purwanto@budiluhur.ac.id[2)]

Abstrak

CV. Felitechno Mandiri adalah sebuah perusahaan yang bergerak di bidang software development. Berfokus pada pengembangan aplikasi web dan hospital asset maintenance management system. permintaan yang banyak dari client untuk pembuatan aplikasi. CV. Felictecho Mendiri berkeinginan membuat aplikasi pertukar pesan (chatting) yang client dapat gunakan. Fitur yang harus tersedia adalah fitur keamanan dalam database guna menungkatkan keamanan pertukaran informasi dalam aplikasi ini. Pada penulisan algoritma yang digunakan adalah kriptografi Caesar Cipher dan 3DES untuk enkripsi dan deskripsi pesan yang tersimpan di dalam database. Dengan metode enkripsi dan deskripsi Caesar Cipher dan 3DES spesan yang disiimpan ke dalam database diubah isi dari plaintext menjadi ciphertext, sehingga informasi data dan kerahasian terjaga. Teknik yang digunakan yaitu teknik kriptografi dengan menggunakan algoritma Caesar Cipher dan 3DES untuk mengenkripsi dan mendeskripsi pesan tersebut. Hasil dari implementasi algoritma Caesar Cipher dan 3DES pada CV. Felichtecho Mandiri bisa membantu proses keamanan pesan pada aplikasi chatting untuk client nantinya.

Kata kunci: Chatting, Caesar Cipher, 3DES, Kriptografi

1. PENDAHULUAN

1.1. Latar belakang

Aspek penting dari suatu sistem informasi adalah masalah keamanan dan kerasiaan data. Jika disadap atau dibajak informasi akan tidak berguna lagi. CV. Felitechno Mandiri adalah sebuah perusahaan yang bergerak di bidang *software development*, berfokus pada pengembangan aplikasi *web* dan *hospital asset maintenance management system*. Untuk menjaga keamanan informasi dan data tersebut perlu proses enkripsi setelah itu proses dekripsi. Beberapa algoritma digunakan untuk melibatkan proses enkripsi dan dekripsi. Berdasarkan pernyataan di atas, untuk meminamalisir dampak kebocoran perlu ada suatu aplikasi pengamanan informasi dalam sebuah data. Maka penulis membuat aplikasi kriptografi *chatting* dengan metode 3DES dan Caesar Cipher berbasis web pada CV. Felitechno Mandiri.

1.2. Batasan Masalah

Batasan masalah pada perancangan aplikasi ini adalah:

1. File yang terenkripsi yaitu data yang disimpan dalam *database*
2. Proses enkripsi menggunakan algoritma Caesar Cipher dan 3DES

1.3. Permasalahan

Dari hasil penelitian dan analisa sistem yang sedang berjalan, ditemukan beberapa masalah:

1. Bagaimana sebuah aplikasi yang terintegrasi langsung ke aplikasi *chatting* dapat menjaga keamanan yang dikirim maupun yang diterima?
2. Bagaimana mengimplementasikan pertukaran data secara *real-time*?
3. Bagaimana sebuah metode kriptografi Caesar Cipher dan 3DES bisa diimplementasikan ke dalam sebuah aplikasi *chatting*?

1.4. Tujuan Penulisan

Tujuan dan maksud bagi penulis adalah untuk mengimplementasikan algoritma kriptografi Caesar Cipher dan 3DES. Sedangkan, bagi CV. Felitechno Mandiri adalah untuk menyediakan produk aplikasi *chatting* yang menggunakan enkripsi dalam melakukan pertukaran data atau komunikasi antar pengguna untuk meningkatkan keamanan data secara *real time*.

2. METODE PENELITIAN

Dalam penyusunan laporan ini penulis menggunakan metode *Waterfall* yang memiliki langkah-langkah sebagai berikut:

2.1. Analisa

Pada tahapan ini dilakukan wawancara kepada Bapak Fadillah Amin selaku *General Manager* untuk mendapatkan Informasi yang dibutuhkan dalam pembuatan aplikasi keamanan *chatting* berbasis *web*, guna mengetahui data apa yang harus diamankan.

2.2. *Design*

Pada tahap *desain* sistem ini dilakukan kegiatan mencari *hardware* dan sistem operasi yang optimal untuk implementasi aplikasi, serta

mendesign sistem yang akan dibuat sepeti database dan rancangan layar untuk memudahkan dalam pengkodingan.

2.3. *Coding* dan *testing*

Pada tahap *coding* dilakukan kegiatan penerjemahan dari rancangan sistem ke dalam bentuk code dengan menggunakan bahasa pemrograman berbasis PHP dan juga menggunakan algoritma Caesar Cipher dan 3DES sebagai pengamanan pesan enkripsi dan deskripsi. Untuk *database*nya sendiri penulis mengunakan aplikasi MySQL.

2.4. Penerapan

Dalam tahap ini penulis mengimplementasikan dan memberikan training penggunaan aplikasi enkripsi *chatting* berbasis *web* yang telah selesai dibuat. Implementasi dan pelatihan ini dilakukan di CV. Felitechno Mandiri.

3. HASIL DAN PEMBAHASAN

3.1. Analisa dan penyelesaian masalah

Dari uraian permasalahan di atas, dengan menggunakan kriptografi aplikasi dapat menjaga kerahasia pesan (*text*) sehingga tidak semua orang bisa melihat isi pesan tersebut. Kerahasiaan pesan menjadi faktor penting karena apabila pesan tersebut diketahui pihak lain yang tidak bertanggung jawab maka pesan dapat diketahui dan merugikan perusahaan. Oleh karna itu aplikasi keamanan data sangat dibutuhkan untuk melindungi keamanan data, sehingga solusi yang tepat adalah dengan menggunakan algoritma kriptografi *Caesar Cipher* dan 3DES digunakan untuk keamanan data pada *database*

3.2. Rancangan basis data

Rancangan basis data yang digunakan dalam penelitian ini adalah:

a. Nama Tabel : users
Primary Key : user_id

Tabel 1. Tabel *users*

No	Nama Field	Type	Panjang	Keterangan
1.	Users_id	Integer	5	Id pengguna
2.	Users_nama	Varchar	100	Nama pengguna
3.	Users_password	Varchar	100	Password pengguna
4.	Users_flag	Tiny integer	1	Flag user yang online

b. Nama Tabel : chat
Primary Key : chat_id

Tabel 2. Tabel *chat*

No	Nama Field	Type	Panjang	Keterangan
1.	Chat_id	Integer	5	Id chat
2.	Users_form	Integer	5	Id pengirim
3.	Chat_text	Text	255	Chat pengguna
4.	Chat_tanggal	Time Stamp		Tanggal chat
5.	User_to	Integer	5	Id penerima
6.	Chat_flag	Tiny integer	1	Flag user yang belum terbaca

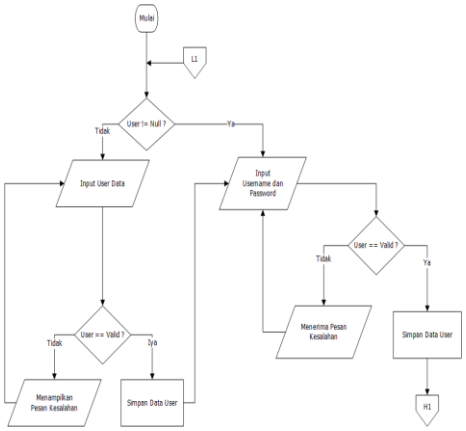
3.3. *Flowchart* dan algoritma

Untuk menyederhanakan, menggambarkan, rangkaian prosedur atau proses sehingga mudah dilihat dan dipahami berdasarkan urutan langkah dari suatu proses bentuk *flowchart* dan algoritma sebagai berikut :

a. Flowchart dan algoritma halaman *register* dan *login*

Pada gambar 5 dapat di jelaskan bahwa proses awal yang harus di lakukan oleh *user* dalah masuk ke dalam halaman utama, jika *user* belum memiliki *userid* maka harus mendaftar terlebih dahulu atau proses *register*, halaman *register user* wajib mengisi *username* dan *password* sebagai syarat untuk masuk ke dalam aplikasi ini, setelah proses *register* selesai *user* akan langsung dibawa ke halaman *login* yang dimana harus mengisi *username* dan *password* yang sesuai dengan yang didaftarkannya.

Kemudian *user* langsung masuk ke halaman menu utama setelah proses *login*.



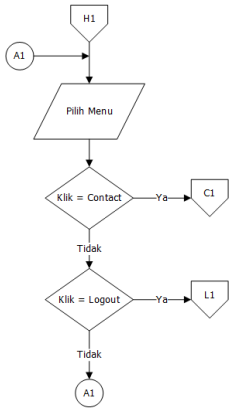
Gambar 1. Flowchart halaman register dan login

Berikut adalah algoritma dari *flowchart* halaman register dan *login* :

```
1.  Mulai
2.  If     username != Null then
3.         Input Username dan Password
4.         If      user == valid then
5.                 Simpan Data User
6.                 Menuju ke halaman Home
7.         Else
8.                 Menampilkan          pesan
    kesalahan
9.                 Kembali ke baris 3
10.        End if
11. Else
12.        Input User Data
13.        If      user == valid then
14.                Simpan Data User
15.                Kembali ke baris 3
16.        Else
17.                Menampilkan          pesan
    kesalahan
18.                Kembali ke baris 12
19.        End if
20. End If
```

b. Flowchart dan algoritma halaman *home*

Berikut adalah *flowchart* dan algoritama halaman *home* :



Gambar 2. Flowchart halaman home

Halaman *home* terdapat beberapa pilihan menu yaitu, menu *contact* dan menu *logout* yang dimana keduanya memiliki fungsi:

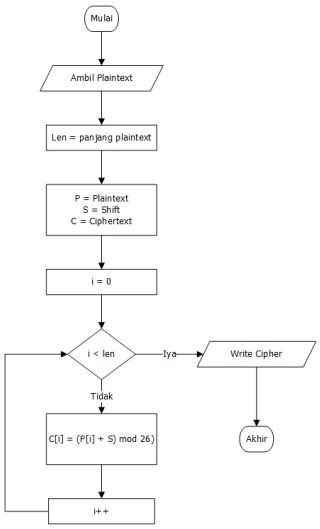
1. Menu *contact* berfungsi untuk memilih teman yang ingin bertukar pesan atau chatting
2. Menu *logout* berfungsi untuk keluar dari aplikasi

Berikut adalah algorima dari halaman *home*:

```
1.  Tampilan halaman home
2.  Pilih Menu
3.  If          klik=contact then
4.              Tampilkan halaman Chatting
                Pengiriman Pesan
5.  Else if     klik=logout then
6.              Tampilkan halaman Login
7.  Else
8.              Kembali ke baris 2
9.  End if
```

c. *Flowchart* dan algoritma proses enkripsi *Caesar Cipher*

Berikut adalah *flowchart* dan algoritma proses enkripsi *Caesar Cipher* :



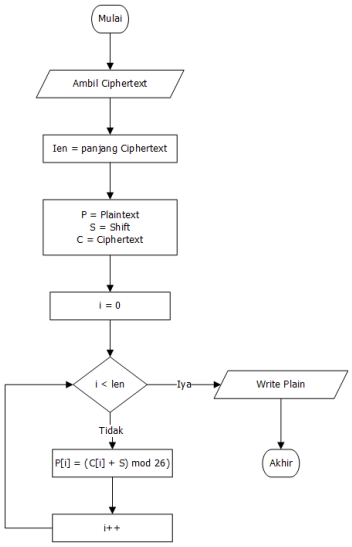
Gambar 3. *Flowchart* proses enkripsi *Caesar Cipher*

Berikut adalah algorima dari *flowchart* proses enkripsi *Caesar Cipher* :

```
1.  Mulai
2.  Ambil plaintext
3.  Len = panjang plaintext
4.  P = plaintext, S = Shif, C = Ciphertext
5.  i = 0
6.  If      i < len then
7.          Write cipher
8.  Else    c[i] = (P[i] + S) mod 26
9.          i ++
10.         Kembali ke baris 6
11. End if
```

d. *Flowchart* dan algoritma proses deskripsi *Caesar Cipher*

Berikut adalah *flowchart* dan algoritma proses deskripsi *Caesar Cipher* :



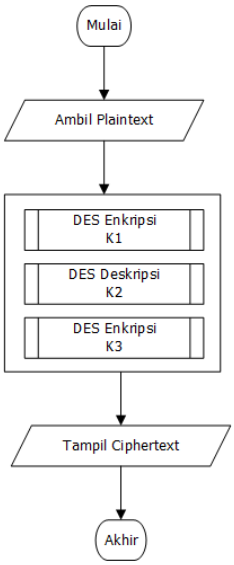
Gambar 4. Flowchart proses dekripsi Caesar Cipher

Berikut adalah algorima dari *flowchart* proses deskripsi *Caesar Cipher* :

1. Mulai
2. Ambil Ciphertext
3. Len = panjang Cipertext
4. P = plaintext, S = Shif, C = Ciphertext
5. i = 0
6. If i < len then
7. Write plant
8. Else c[i] = (P[i] + S) mod 26
9. i ++
10. Kembali ke baris 6
11. End if

e. *Flowchart* dan algoritma proses enkripsi 3DES

Berikut adalah *flowchart* dan algoritama proses enkripsi 3DES :



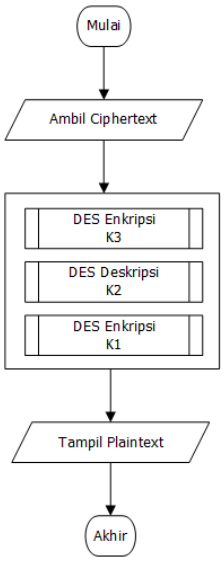
Gambar 5. Flowchart proses enkripsi 3DES

Berikut adalah algorima dari *flowchart* proses enkripsi 3DES:

1. Mulai
2. Ambil plaintext
3. DES enkripsi K1 then
4. DES enkripsi K2 then
5. DES enkripsi K3 then
6. Tampil chipertext
7. Akhir

f. *Flowchart* dan algoritma proses deskripsi 3DES

Berikut adalah flowchart dan algoritama proses deskripsi 3DES :



Gambar 6. Flowchart proses deskripsi 3DES

Berikut adalah algorima dari *flowchart* proses deskripsi 3DES:

1. Mulai
2. Ambil cipertext
3. DES enkripsi K3 then
4. DES enkripsi K2 then
5. DES enkripsi K1 then
6. Tampil plaintext
7. Akhir

3.4. Implementasi dan ujicoba aplikasi

a. Implementasi program

Implementasi program berfungsi untuk mengetahui maksimal atau tidakh program yang telah dibuat sehingga tidak terjadi kesalahan-kesalahaa, ujicoba program harus dilakukan agar dapat berjalan sesuai dengan yang diharapkan pada saat implementasi nantinya.

b. Hasil uji aplikasi

1) Tampilan halaman menu utama (*login*)

Halaman awal pada aplikasi *chatting* ini adalah halaman *login*. Halaman *login* akan menampilkan kolom *username* dan *password*, *username* adalah *userid* yang terlah didaftarkan sebelumnya oleh *user* tersebut sama dengan *password*, berikut tampilan menu utamanya :

Gambar 7. Tampilan halaman utama (login)

2) Tampilan halaman *register*

Berikut adalah tampilan halaman *register*. Pada halaman ini terdapat kolom untuk mendaftarkan pengguna baru agar dapat menggunakan aplikasi *chatting* ini.

Gambar 8. Tampilan halaman register

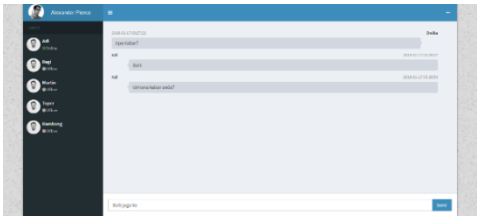
3) Tampilan halaman home

Setelah berhasil melakukan proses *login*, *user* akan dipindahkan ke halaman *home*. Pada halaman ini terdapat menu-menu yang dapat diakses oleh user yaitu *home*, notifikasi, dan *sign out*.

Gambar 9. Tampilan halaman home

4) Tampilan halaman *chatting* pengirim pesan

Berikut adalah pengujian halaman chatting pengirim pesan. Setiap pesan yang dikirim dan diterima akan tampil di layar *chatbox*. Terdapat waktu untuk mempermudah pengguna melihat kapan pesan *chatting* tersebut dikirim maupun diterima.



Gambar 10. Tampilan halaman chatting pengirim pesan

c. Tabel pengujian

1) Tabel pengujian proses enkripsi

Berikut adalah tabel pengujian proses enkripsi :

Tabel 3. Tabel pengujian proses enkripsi

No	Pengirim	Plaintext	Penerima	ciphertext
1.	user1	hi, salam kenal	user2	LXPly3PlO4U0Os/wj5Y0ug==
		saya dwika mahasiswa budi luhur		O4N3i+UDCfeWN4OMSjr4eu8YH53AyNfTDVBwT4AA+I4=
		boleh berkenalan?		U8M3tfrjmlFcMXzEzHm18nIf15cbqt3R
2.	user2	Boleh, nama saya arief	user1	jUnleMCHlyFcYZTyiTLfgo1Y9uZIfGgT
		Saya juga mahasiswa budi luhur		9TWvKQMLhMvgjgZuCqUOjCsNFeXHBlqPVRrdre0MrLY=
		Kamu fakultas apa		AOzMmzdpSiOC4lG2I3W+N3AfQXKJDWUa

2) Tabel pengujian proses deskripsi

Berikut adalah tabel pengujian proses deskripsi chatting :

Tabel 4. Tabel pengujian proses deskripsi

No	Penerima	Ciphertext	Plaintext
1.	user1	LXPly3PlO4U0Os/wj5Y0ug==	hi, salam kenal
		O4N3i+UDCfeWN4OMSjr4eu8YH53AyNfTDVBwT4AA+I4=	saya dwika mahasiswa budi luhur
		U8M3tfrjmlFcMXzEzHm18nIf15cbqt3R	boleh berkenalan ?
2.	user2	jUnleMCHlyFcYZTyiTLfgo1Y9uZIfGgT	Boleh, nama saya arief
		9TWvKQMLhMvgjgZuCqUOjCsNFeXHBlqPVRrdre0MrLY=	Saya juga mahasiswa budi luhur
		AOzMmzdpSiOC4lG2I3W+N3AfQXKJDWUa	Kamu fakultas apa

d. Evaluasi sistem

Setelah dilakukan evaluasi sistem pengujian aplikasi chatting ini, terdapat berberapa kelebihan dan kekurangan, yaitu sebagai berikut:

1) Kelebihan aplikasi

a) Aplikasi Dapat digunakan di semua personal komputer yang terhubung dengan *server*, sehingga lebih mudah untuk segala jenis *operating* sistem.
b) Pengiriman pesan sudah secara real time pada aplikasi ini.
c) Untuk *client*, hanya membutuhkan *browser* untuk menjalankan aplikasi *chatting* ini.
d) Aplikasi miliki tampilan yang sederhana sehingga mudah dimengerti oleh para pengguna.

2) Kekurangan aplikasi

a) Hanya text yang dapat di kirimkan pada Aplikasi *chatting* ini.
b) Alamat, nomor telepon dan foto tidak ditampilkan pada pada aplikasi ini.
c) Tidak bias mengubah *username* dan *password* pada aplikasi ini .
d) *History* pesan di dalam *chatbox* tidak dapat dihapus.

4. KESIMPULAN

Dengan adanya implementasi kriptografi *Caesar Cipher* dan 3DES (3DES) pada aplikasi *chatting*, maka penulis dapat mengambil kesimpulan bahwa :

1) Algoritma kriptografi *Caesar Cipher* dapat dikombinasikan dengan algoritma 3DES pada aplikasi *chatting* berbasis *web*.
2) Aplikasi chatting berbasi *web* ini pengamanan datanya menggunakan kriptografi.
3) Dengan diterapkan algoritma *Caesar Cipher* dan 3DES pada proses enkripsi dan deskripsi pengiriman data, data yang tersimpan dalam *database* tidak dapat dimanupulasi oleh pihak luar yang tidak memiliki wewenang.

5. DAFTAR PUSTAKA

[1] Ariyus, D. (2008) 'Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi'.
[2] Haryanto, H., Wiryadinata, R. and Afif, M. (2014) 'Implementasi Kombinasi Algoritma Enkripsi Aes 128 Dan Algoritma Kompresi Shannon-Fano', Setrum, 3(1), pp. 16–25.
[3] Kromodimoeljo, Sentot (2009). Teori dan Aplikasi Kriptografi, Teori, Aplikasi, dan kriptografi. ISBN 978-602-96233-0-7, SPK IT Consulting.