Jurnal Politeknik Caltex Riau
http://jurnal.pcr.ac.id

Sistem Keamanan Aplikasi Chatting Menggunakan Algoritma Camelia

Srimuliyani S.ST[1], Wiwin Styorini, S.T.,M.T[2] ,Wahyuni Khabzli, S.T.,M.T[3]

[1]Politeknik Caltex Riau, email: sri@mahasiswa.pcr.ac.id
[2]Politeknik Caltex Riau, email: wiwin@pcr.ac.id
[3]Politeknik Caltex Riau, email: ayu@pcr.ac.id

Abstrak

Perkembangan teknologi sekarang ini sangat penting dalam pengiriman suatu informasi, Sehingga menyebabkan tingginya tingkat resiko dalam penyadapan data. Salah satu cara untuk mengamankan dari penyadapan tersebut dengan menggunakan metode kriptografi. Dimana data atau informasi yang bersifat rahasia agar tidak diketahui oleh pihak-pihak yang tidak berkepentingan. Salah satu metoda kriptografi yang di gunakan yaitu metode camellia. Camellia merupakan block chiper yang di rancang oleh ahli-ahli dalam riset dan pengembangan teknik kriptografi.. Metode camellia memiliki 3 secret kunci yaitu 128-bit, 192-bit, dan 256-bit, dan dengan blok data sebesar 128-bit. Aplikasi ini menggunakan bahasa pemograman PHP. Pada penelitian ini juga menambahkan sebuah web untuk aplikasi chatting menggunakan algoritma camellia. Hasil yang didapat dalam penelitian ini menunjukkan bahwa proses enkripsi dengan algoritma camellia dapat dikembalikan lagi dengan deskripsi menggunakan kunci yang sama. Untuk waktu enkripsi menggunakan panjang kunci 256 bit yaitu 0.092s dan *jumlah blok hasil chiperteks berbanding lurus dengan jumlah blok plainteksnya.*

Kata kunci: *Camellia, kriptografi, enkripsi, Dekripsi, PHP (Perl Hypertext Processor)*

Abstract

Current technological development is very important in the delivery of an information. Thus leading to high levels of piracy risk in the data. One way to safeguard against piracy data using cryptographic methods. Where data or confidential information that is not known by the parties who are not interested. One method of cryptography in use is the method camellia. Camellia is a block cipher designed by experts in the research and development of cryptographic techniques. Method camellia has three secret key is 128-bit, 192-bit and 256-bit, and the data blocks of 128-bit. This application uses the programming language PHP. At the end of this project adds to build a web chat application using algorithms camellia. At the end of this project can be concluded, for the longer time encryption using 256 bit key length, and managed to build web applications using algorithms camellia chat.

Keywords: *Camellia, Cryptograpy, Encryption, Decryption, PHP (Perl Hypertext Processor*

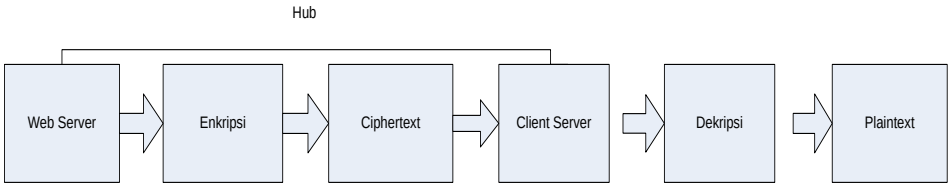
Dokumen diterima pada 25 Juni, 2016
Dipublikasikan pada 30 November, 2016

1. Pendahuluan

Berkembangnya teknologi dapat dilihat dalam kehidupan sehari-hari, salah satu contohnya yaitu masalah keamanan data. Dimana dalam proses pengiriman data sangat mudah dilakukan oleh seseorang melalui berbagai macam media yang ada. Hal ini diperlukan pengamanan data terutama pada saat pengiriman data dari seseorang kepada orang lain. Pada saat pengiriman sering terjadinya penyadapan. Salah satu cara untuk mengatasi keamanan data yaitu menggunakan kriptografi. Dimana kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami pemyadapan dari pihak-pihak yang tidak berkepentingan.

Salah satu metode kriptografi yang bisa diterapkan adalah metode camellia.. pada penelitian ini algoritma camellia diterapkan untuk keamanan data pada aplikasi *chatting*. Terdapat tiga tahapan proses yaitu pembentukan kunci untuk menghasilkan kunci efektif berdasarkan kunci atau *password* yang dimasukkan oleh user, dilanjutkan dengan proses enkripsi yaitu proses mengubah pesan yang dapat dibaca menjadi pesan dalam bentuk lain berdasarkan hasil pembentukan kunci. Sedangkan proses deskripsi merupakan proses untuk membalikkan pesan yang telah terenkripsi menjadi bentuk pesan yang dapat dibaca . Metode camellia diputar dengan menggunakan kunci yang panjangnya 128, 192, 256 bit dan dengan blok data sebesar 128-bit.

2. Perancangan aplikasi

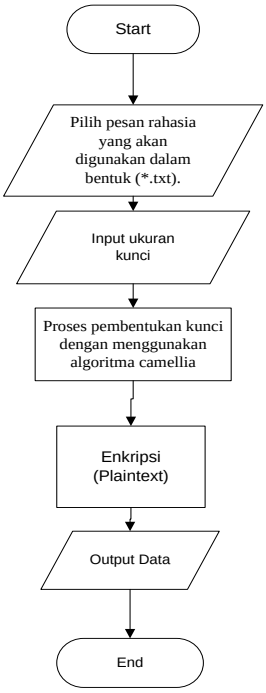


Gambar 1. Blok diagram perancangan aplikasi

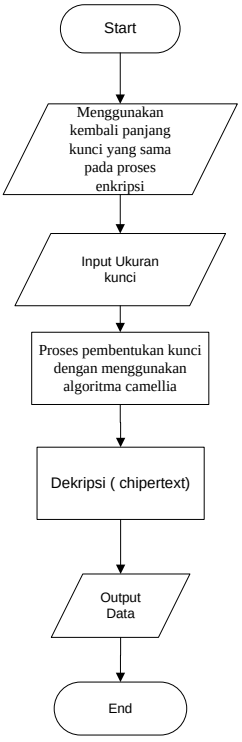
Pada gambar 1 terdapat empat bagian, yaitu *Plaintext* atau pesan asli, enkripsi yaitu proses mengubah pesan asli menjadi pesan yang sudh diacak (*chipertext),* dekripsi yaitu proses mengubah data yang sudah diacak dikembalikan kedata asli.

Pada penelitian ini dirancang dua proses yaitu proses enkripsi dan deskripsi. Pada proses Enkripsi, harus menginput *text file* rahasia yang akan disisipkan yaitu (*.txt). kemudian input ukuran kunci. Selanjutnya proses pembentukan kunci dengan menggunakan algoritma camelia. Dilanjutkan dengan proses enkripsi (mengubah plaintext menjadi chipertext) dengan nilai kunci 128 bit.

Sedangkan pada proses dekripsi adalah proses mengubah *ciphertext* menjadi *plaintext*. Pada proses dekripsi dimulai dengan menggunakan kembali panjang kunci yang sama pada proses enkripsi. Kemudian dilanjutkan dengan proses pembentukan kunci dengan menggunakan algoritma camelia. Setelah itu masuk pada proses dekripsi dengan ukuran dengan ukuran kunci 128 bit, kemudian didapat *output* data berupa *plaintext.* Diagram alir dari proses enkripsi dan deskripsi dapat dilihat pada gambar 2 dan gambar 3.



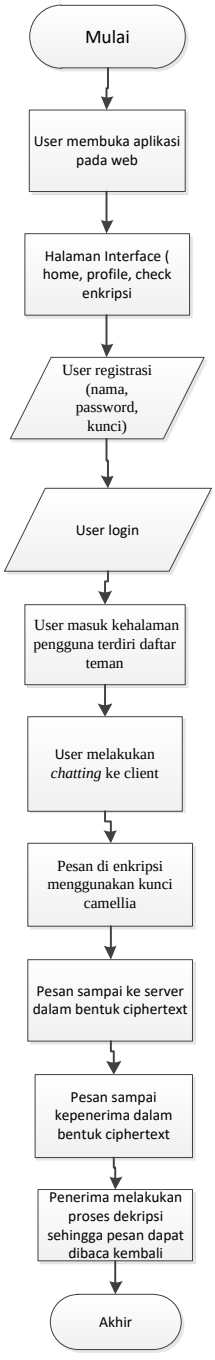
Gambar 2 Diagram alir proses enkripsi



Gambar 3 Diagram alir proses deskripsi

Untuk diagram alir dari aplikasi pada sistem keamanan data ini dapat dilihat pada diagram alir yang ditunjukkan pada gambar 4. Dimana pada aplikasi ini menggunakan dua PC yaitu sebagai

server dan *client*. Pada proses pertama *user* membuka wamp *serv*er untuk membuka halaman web. Setelah masuk ke aplikasi akan muncul tampilan awal aplikasi chatting. yang terdiri dari menu *home, chat,* registrasi, proses selanjutnya *user* akan melakukan registrasi yang akan disimpan kedalam database. Kemudian login untuk masuk ke aplikasi, maka akan muncul halaman pengguna, pengguna dapat memilih salah satu dari daftar nama yang dipilih untuk melakukan proses chatting kemudian *user* melakukan chatting ke *client* dengan hasil *chipertext* sampai ke penerima dengan hasil *ciphertext* (data acak) kemudian akan di dekripsi sehingga pesan dapat dibaca *(plaintext)*.



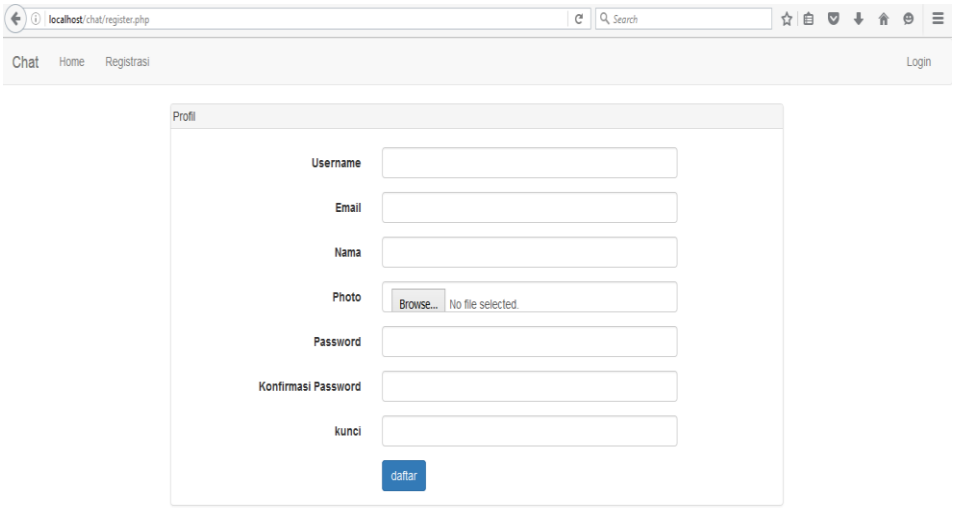
Gambar 4 Diagram alir aplikasi secara keseluruhan

3. Hasil Dan Pembahasan

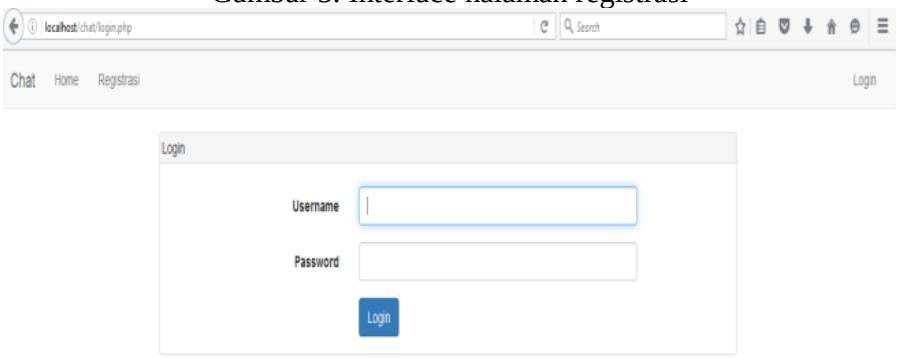
Pada bagian ini akan dilakukan pengujian dan analisa terhadap aplikasi kriptografi menggunakan algoritma Camelia untuk sistem keamanan data pada aplikasi chatting.

3.1. Interface dari aplikasi

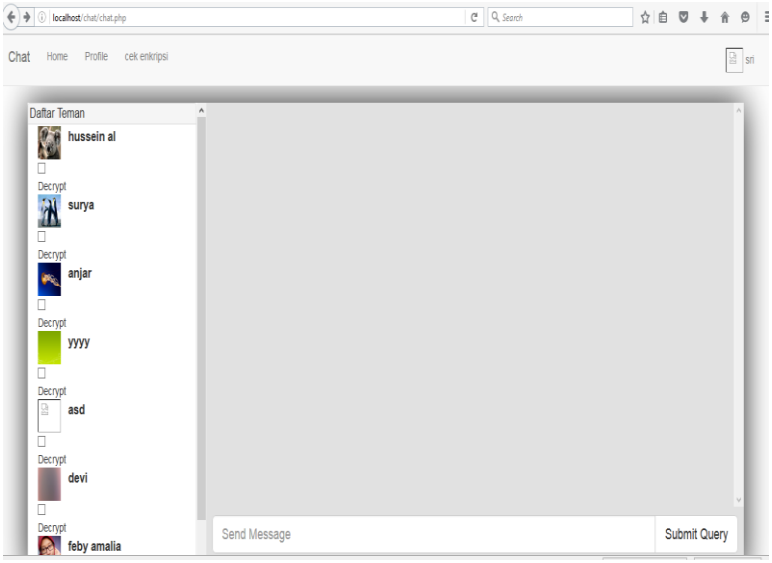
Interface untuk aplikasi ini terdiri dari halaman registrasi, halaman login, halaman awal, halaman chatting. Masing-masing dapat dilihat pada gambar 5, gambar 6, gambar 7, gambar 8.



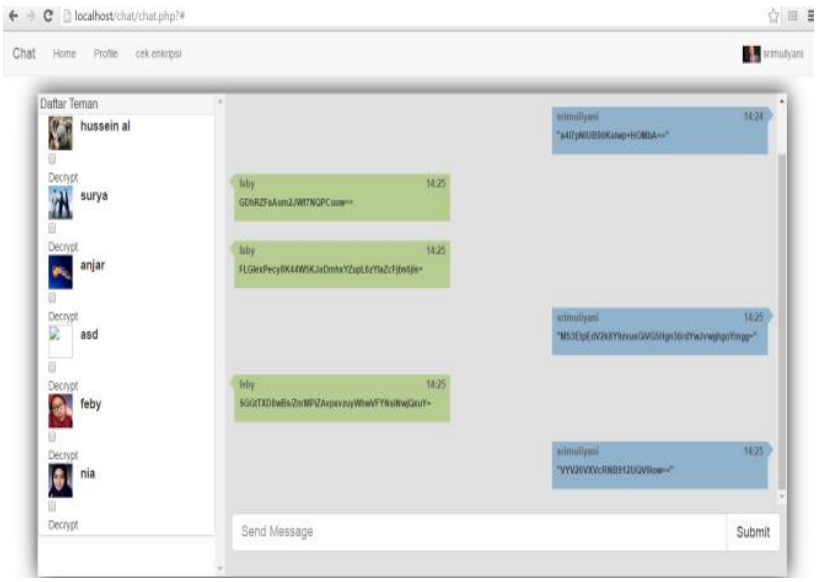
Gambar 5. Interface halaman registrasi



Gambar 6. Interface halaman login



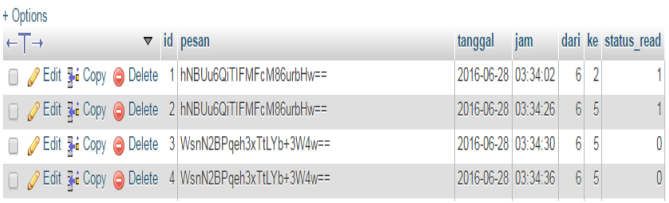
Gambar 7. Interface halaman awal



Gambar 8. Interface halaman chating

3.2 Database pada server

d*atabase* yang terdiri dari beberapa tabel yang didalamnya sudah terdapat nama-nama *field* yang telah di tentukan. Cara merancang relasi antar tabel yaitu menggunakan halaman PhpMyAdmin dengan masuk ke alamat "*localhost/phpmyadmin",* kemudian klik database yang akan dibuat. Database ini yang dibuat yaitu *chat* dan *nama user.*



Gambar 9. Database hasil enkripsi server online

3.3. Pengujian enkripsi dan dekripsi

Pada bagian ini akan membahas hasil pengujian dari proses enkripsi dan dekripsi dilihat dari :

1. Waktu perbandingan menggunakan panjang kunci 192, 192, 256 enkripsi dan dekripai.
2. Hasil enkripsi berupa chipertext hingga menjadi plaintext.
3. Pengujian keamanan isi pesan.

3.3.1 Pengujian perbandingan panjang kunci pada algoritma camellia

Dalam pengujian untuk waktu enkripsi dan dekripsi menggunakan panjang kunci 128, 192, 256, terlihat waktu yang signifikan, semakin panjang kunci yang dimasukkan , maka waktu enkripsi dan dekripsi akan semakin lama. Kunci dengan panjang 128 bit lebih cepat untuk waktu enkripsi dan dekripsi.

Tabel 1. Perbandingan waktu enkripsi

No	Panjang kunci algoritma Camellia	Pesan	Waktu enkripsi (ms)
1.	128 bit	makan	0.014
2.	192 bit	makan	0.057
3.	256 bit	makan	0.092

Pada table 1 didapat hasil plainteks menjadi *chipertext* dengan panjang karakter pesan yang sama dengan panjang kunci yang berbeda, hasil waktu yang didapat tidak jauh berbeda, untuk panjang kunci 256 didapat 0,092ms.

3.4.2 Pengujian keamanan isi *chatting*

Dalam pengujian keamanan chatting dengan algoritma camellia dapat terjaga kerahasiaannya, dapat dilihat pada gambar 10, dari pesan enkripsi yang dikirimkan dan pesan hasil dekripsi melalui aplikasi ini tersimpan didalam database. Selain itu, pesan yang dienkripsi (*ciphertext*) tidak bisa dibaca atau diubah ke pesan aslinya (*plaintext*) tanpa mengetahui atau memasukkan kunci yang benar.

Gambar 10. Hasil enkripsi pada aplikasi chatting

4. Kesimpulan

1. Kecepatan waktu enkripsi dan dekripsi lebih lama menggunakan Panjang kunci 256 bit yaitu 0.092 ms
2. Jumlah blok hasil chiperteks berbanding lurus dengan jumlah blok plainteks. Semakin banyak teks yang dikirim semakin banyak pula jumlah chiperteksnya.
3. Aplikasi ini juga telah berhasil mengembalikan file yang telah diacak tersebut (cipherteks) seperti semula dengan menggunakan kunci yang sama sewaktu enkripsi.

5. Daftar Pustaka

[1] Ahmad Rosyadi, " Implementasi Algoritma Kriptografi AES untuk Enkripsi dan Dekripsi Email", *Univ. Dipenogoro Semarang.*

[2] Seti Fauziah, " Studi Enkripsi dan Dekripsi File dengan menggunakan algoritma Twofish*", Univ. Sumatera Utara*, 2009.

[3] Suriski Sitinjak, Fauziah Yuli, Juwariah, " Aplikasi Kriptografi File menggunakan Algoritma Blowfish", *UPN" Veteran" Yogyakarta, 2010.*

[4] Munir, Rinaldi. (2006) *Kriptografi*. Bandung. *Jurnal TeknikInformatika Universitas Kristen Petra.*