Penerapan Algoritma Elgamal dan SSL Pada Aplikasi Group Chat

Heru Aditya[1], Intan Nur Farida[2], Risky Aswi Ramadhani[3]
[1,2,3]Teknik Informatika, Fakultas Teknik, Universitas Nusantara PGRI Kediri
E-mail: *[1]*aytidaureh@gmail.com, in.nfarida@gmail.com* [2], [3] *ra.komo999@gmail.com*

Abstrak – *Seiring dengan pesatnya perkembangan jaman dan majunya teknologi saat ini membawa pengaruh besar pada aspek kehidupan manusia, salah satu contohnya adalah dalam hal komunikasi. Chatting merupakan salah satu pilihan dalam berkomunikasi. Tujuan yang hendak ingin dicapai adalah membuat sebuah aplikasi group chat dengan menerapkan algoritma kriptografi elgamal pada database pesannya dan SSL pada pengamanan jaringannya. Teknik penelitian dalam penelitian ini adalah Penelitian Pengembangan atau Rekayasa Teknologi Informasi dengan subyek dosen wali dan mahasiswa kelas 4G angkatan 2013 Prodi Teknik Informatika Universitas Nusantara PGRI Kediri. Dari penelitian ini telah dihasilkan aplikasi grup chat. Aplikasi ini dibuat dengan menggunakan bahasa php, script jquery, dan database mysql. Berdasarkan penelitian direkomendasikan: (1) Aplikasi perlu ditambah menu pengiriman berupa gambar, file dan emoticon. (2) Aplikasi perlu dirubah script jquerynya agar dapat dijalankan secara online. (3) Aplikasi perlu ditambahi fitur private chat sehingga dapat melakukan komunikasi dengan member lain satu per satu.*

Kata Kunci *— Chat, Elgamal, Keamanan Jaringan, Kriptografi, SSL*

Abstract – *Along with the rapid development of the times and the advancement of technology today brings great influence on aspects of human life, one example is in terms of communication. Chatting is one option in communicating. The goal is to create a group chat application by implementing the algorithm of elgamal on its message database and use SSL on its network security. Techniques research in this research is Research Development or Engineering Information Technology with the subject of guardian lecturers and students of 4G class 2013 Informatics Engineering University of Nusantara PGRI Kediri. From this research has generated chat group application. This application is created using php language, jquery script, and mysql database. Based on the research recommended: (1) Application Consultation need plus menu delivery in the form of picture, file and emoticon. (2) The application needs to be changed jquery script to be run online. (3) The application needs to be added private chat feature so that it can communicate with other member one by one.*

Keywords *— Chat, Cryptography, Elgamal, Network Security, SSL*

1. PENDAHULUAN

Seiring dengan pesatnya perkembangan jaman dan majunya teknologi saat ini membawa pengaruh besar pada aspek kehidupan manusia, salah satu contohnya adalah dalam hal komunikasi Berbagai macam penunjang komunikasi telah bermunculan seperti telepon genggam sampai internet sehingga kita dapat dengan mudah berkomunikasi dengan orang lain. Chatting merupakan salah satu pilihan dalam berkomunikasi. Isi dari percakapan chatting bersifat rahasia sehingga diperlukan keamanan untuk melindungi isi percakapan tersebut. Tak sedikit orang yang berbuat curang untuk mencari tahu isi percakapan tersebut. Dengan melakukan sniffing ataupun sql injection penyerang dapat melakukan pencurian informasi. Sniffing adalah teknik menangkap paket data dalam satu jaringan[1]. Dengan menggunakan tool sniffing seperti wireshark penyerang dapat menangkap paket data berupa isi percakapan di dalam chatting. Melihat berbahayanya dampak dari sniffing dan sql injection maka dari itu diperlukan algoritma kriptografi dan SSL. Salah satu algoritma kriptografi itu adalah algoritma ElGamal. Elgamal akan melindungi pesan yang ada di database dari sql injection dan SSL mengamanan proses pengiriman pesan dalam jaringan. Penelitian ini diambil

dengan mengembangkan penelitian terdahulu salah satunya seperti pada paper milik Yudhistira Taufan A. (2011) yang berjudulkan: "Enkripsi Email Dengan Menggunakan Metode Elgamal Pada Perangkat Mobile" [2]. Pengembangannya dengan menerapkan Elgamal pada aplikasi Group Chat.

2. METODE PENELITIAN

2.1. Analisa Sistem

Spesifikasi kebutuhan fungsional dari perangkat lunak untuk sistem ini adalah :

1. Data Set mengenai informasi berupa npm/nidn, nama dan password mahasiswa kelas 4G dan juga nilai yang dibutuhkan dalam algoritma elgamal seperti nilai prima, nilai primitif dan kunci rahasia.
2. Data Testing, digunakan untuk melakukan testing data untuk menguji sistem saat dijalankan. Data testingnya berupa teks (pesan).

2.1. Agoritma Elgamal

Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan [3].

2.1.1 Proses Pembentukan Kunci

Pembentukan kunci terdiri atas pembentukan kunci publik dan kunci rahasia. Pada proses ini dibutuhkan sebuah bilangan prima p yang digunakan untuk membentuk grup Zp*, elemen primitif α dan sembarang.

$$a \in \{0,1,..., p-2\} \quad \text{..... (1)}$$

Kunci publik algoritma ElGamal terdiri atas pasangan 3 bilangan (p,α ,β) dimana

$$\beta = \alpha^a mod\ p \quad \text{..... (2)}$$

Sedangkan kunci rahasianya adalah bilangan a tersebut.
Proses pembentukan kunci untuk algoritma ElGamal terdiri atas:

2.1.2 Penentuan Bilangan Prima Aman Yang Bernilai Besar

Tujuan penentuan bilangan prima aman ini adalah untuk mempermudah dalam penentuan elemen primitif. Digunakan bilangan prima p sehingga

$$p = 2.q + 1 \quad \text{..... (3)}$$

Langkah penentuan bilangan prima tersebut dinyatakan sebagai berikut:

1) Tentukan bilangan prima p ≥ 5
2) Hitung q dengan "persamaan (2)"
3) Jika q merupakan bilangan prima, maka p merupakan bilangan prima aman.
4) Jika q bukan merupakan bilangan prima, maka p bukan merupakan bilangan prima aman.

2.1.3 Penentuan elemen primitive

Teorema: "Suatu elemen yang membangun Zp * disebut elemen primitif (primitive root) mod p". "Bila $\alpha^2\ mod\ p \neq 1\ atau\ a^q mod\ pp \neq 1$. Jika keduanya dipenuhi, maka α adalah elemen primitif dari Zp *."
Langkah penentuan elemen primitif tersebut dapat dinyatakan sebagai berikut:

1) Tentukan bilangan prima $p\ \geq 5\ dan\ \alpha \in Zp*$
2) Hitung q dengan "persamaan (2)"
3) Hitung $\alpha^2 mod\ p$ dan $\alpha^q mod\ p$
4) Jika $\alpha^2\ mod\ p = 1\ atau\ a^q mod\ p = 1$, maka α bukan merupakan elemen primitif.
5) Jika $\alpha^2\ mod\ p \neq 1\ atau\ a^q mod\ pp \neq 1$, maka α merupakan elemen primitif.

2.1.4 Pembentukan kunci berdasarkan bilangan prima aman dan elemen primitive

Setelah bilangan prima aman dan elemen primitif diperoleh, kunci publik dan kunci rahasia untuk algoritma ElGamal dapat dibentuk. Algoritma ElGamal dalam prosesnya menggunakan bilangan bulat untuk perhitungan. Oleh karena itu, pesan yang terkandung dalam plainteks harus dalam bentuk bilangan bulat. Untuk memenuhi persyaratan tersebut, digunakan kode ASCII (American Standard for Information Interchange) yang merupakan representasi numeric dari karakterkarakter yang digunakan pada komputer, serta mempunyai nilai minimal 0 dan maksimal 255.

Selanjutnya, dengan kondisi-kondisi tersebut, pembentukan kunci dapat dibentuk dengan mengacu pada langkah berikut:

1) Tentukan bilangan prima $p \geq 5$ dan $\alpha \in Zp^*$
2) Pilih a $\in \{0,1,..., p-2\}$ sembarang.
3) Hitung nilai β dengan rumus

$$\beta = \alpha^a mod\ p \quad \text{..... (4)}$$

2. Proses Enkripsi

Proses enkripsi menggunakan kunci publik (p,α ,β) dan sebuah bilangan integer acak a (a $\in \{0,1,..., p-1\}$) yang dijaga kerahasiaannya oleh penerima yang mengenkripsi pesan. Untuk setiap karakter dalam pesan dienkripsi dengan menggunakan bilangan k yang berbeda-beda. Satu karakter yang direpresentasikan dengan menggunakan bilangan bulat ASCII akan menghasilkan kode dalam bentuk blok yang terdiri atas dua nilai (r, t). Langkah proses enkripsi:

1) Ambil sebuah karakter dalam pesan yang akan dienkripsi dan transformasi karakter tersebut ke dalam kode ASCII sehingga diperoleh bilangan bulat M.
2) Hitung nilai r dan t dengan persamaan berikut:

$$r = \alpha^a (mod\ p \text{..... (5)}$$

$$t = [\beta]^a M\ (mod\ p) \text{..... (6)}$$

3) Diperoleh cipherteks untuk karakter M tersebut dalam blok (r,t)
4) Lakukan proses di atas untuk seluruh karakter dalam pesan termasuk karakter spasi

3. Proses Dekripsi

Dekripsi dari cipherteks ke plainteks menggunakan kunci rahasia a yang disimpan kerahasiaanya oleh penerima pesan. Teorema: Diberikan (p,α ,β) sebagai kunci public dan a sebagai kunci rahasia pada algoritma ElGamal. Jika diberikan cipherteks (r, t), maka.

$$\text{M} = t(r^a)^{-1} mod\ p \text{ ..... (7)}$$

dengan M adalah plainteks. Di mana nilai

$$(r^a)^{-1} = r^{-a} = r^{p-1-a} mod\ p \text{ ..... (8)}$$

Langkah proses dekripsi :

1) Ambil sebuah blok cipherteks dari pesan yang telah dienkripsikan pengirim.
2) Dengan menggunakan a yang dirahasiakan oleh penerima, hitung nilai plainteks dengan menggunakan “persamaan (7)” dan “persamaan (8)”.

4. Secure Socket Layer

Secure Socket Layer (SSL) adalah protokol yang digunakan untuk browsing web secara aman. SSL bertindak sebagai protokol yang mengamankan komunikasi antara client dan server. Protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara website dan web browser. SSL dikembangkan oleh Netscape Communations pada tahun 1994 [4].

3. HASIL DAN PEMBAHASAN

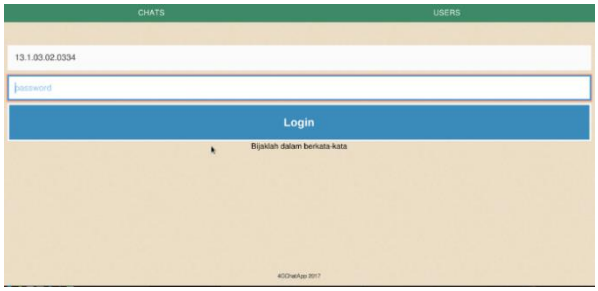
3. Tampilan Program

3.1.1 Halaman Awal Aplikasi Group Chatting

Gambar 1. Halaman Awal Aplikasi Group Chat

Pada halaman awal aplikasi group chat akan disuguhkan penjelasan tentang aplikasi, penggunaan dan link menu halaman login.

3.1.2 Halaman Login Aplikasi Group Chatting



Gambar 2. Halaman Login Aplikasi Group Chat

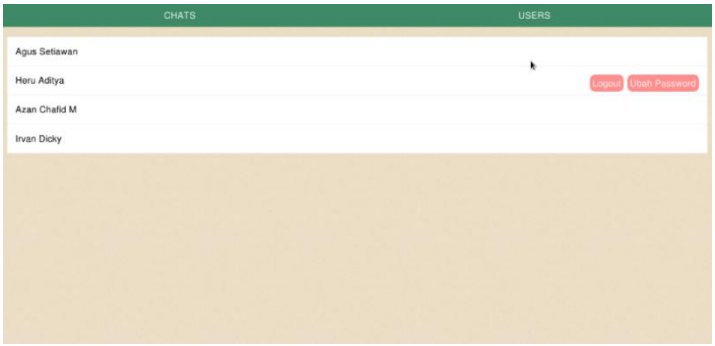
Pada halaman login aplikasi,terdapat form input nidn/npm dan juga password beseta button Login. Button itu digunakan untuk mengirimkan data nidn/npm dan password untuk dicocokkan dengan data yang ada di database tabel “members” dan jika cocok akan mengirimkan nilai field “name” dari nidn/npm yang diinputkan ke field “name” tabel “chatters”.

3.1.3 Halaman Chats Aplikasi Group Chat

Gambar 3. Tampilan Chats

Pada tampilan chats terdapat percakapan dari dosen dan mahasiswa dan juga form input pesan yang siap disamarkan dengan proses enkripsi elgamal. Percakapan yang tampil diambil dari database “chatting” tabel “messages” dan didekripsi menjadi plainteks.

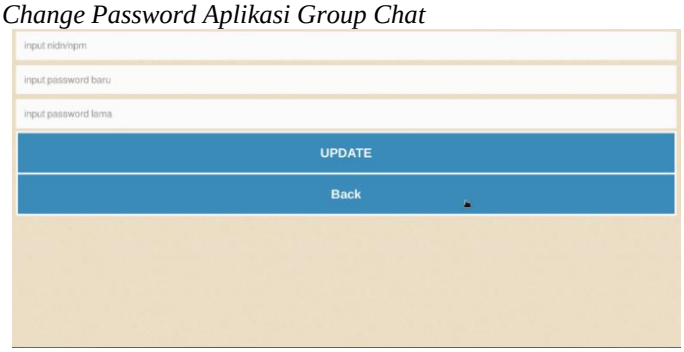
3.1.4 Tampilan Users Aplikasi Group Chat



Gambar 4. Tampilan Users

Tampilan users menampilkan daftar member siapa saja yang online yang diambil dari database “chatters”. Dan juga terdapat button Logout yang berfungsi untuk keluar atau offline dari aplikasi dan button Change Password yang akan mengantarkan kita ke tampilan Change Password.

3.1.5 Tampilan Change Password Aplikasi Group Chat

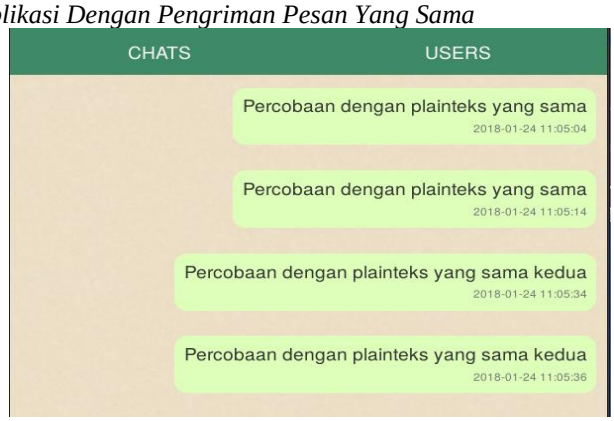


Gambar 5. Tampilan Change Password

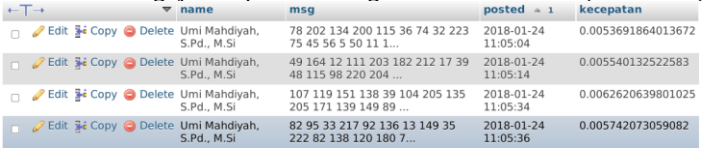
Tampilan change password terdapat form inputan nidn/npm,form inputan password baru,dan inputan password lama, dimana form inputan nidn/npm dan inputan password lama yang digunakan sebagai acuan perubahan password.

3.2 Pengujian

3.2.1 Pengujian Aplikasi Dengan Pengriman Pesan Yang Sama



Gambar 6. Pengujian Aplikasi Dengan Plainteks Sama (interface)



	name	msg	posted	kecepatan
Edit Copy Delete	Umi Mahdiyah, S.Pd., M.Si	78 202 134 200 115 36 74 32 223 75 45 56 5 50 11 1...	2018-01-24 11:05:04	0.0053691864013672
Edit Copy Delete	Umi Mahdiyah, S.Pd., M.Si	49 164 12 111 203 182 212 17 39 48 115 98 220 204 ...	2018-01-24 11:05:14	0.005540132522583
Edit Copy Delete	Umi Mahdiyah, S.Pd., M.Si	107 119 151 138 39 104 205 135 205 171 139 149 89 ...	2018-01-24 11:05:34	0.0062620639801025
Edit Copy Delete	Umi Mahdiyah, S.Pd., M.Si	82 95 33 217 92 136 13 149 35 222 82 138 120 180 7...	2018-01-24 11:05:36	0.005742073059082

Gambar 7. Pengujian Aplikasi Dengan Plainteks Sama (database)

Pengujian pertama yaitu pengujian dengan plainteks yang sama yang di tunjukan pada Gambar 6 dan Gambar 7. Pada Gambar 6 terlihat plainteks yang ditampilkan sama, tapi berbeda dengan hasil enkripsi yang dihasilkan berbeda bisa dilihat pada gambar 5.18 pada field “msg”.

3.2.2 Pengujian Kecepatan Proses ElGamal Dengan Plainteks Yang Sama dan Berbeda

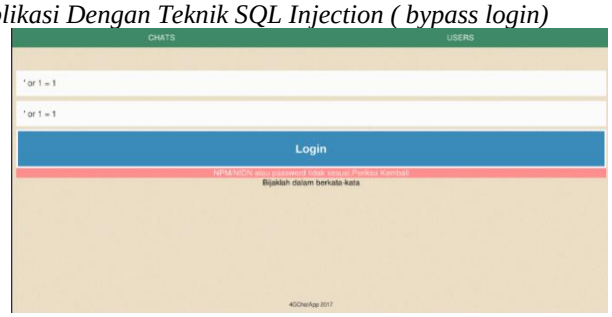
Gambar 8. Pengujian Kecepatan Proses Elgamal (interface)

	name	msg	posted	kecepatan
Edit Copy Delete	Umi Mahdiyah, S.Pd., M.Si	62 116	2018-01-24 11:08:24	0.0025970935821533
Edit Copy Delete	Umi Mahdiyah, S.Pd., M.Si	135 7	2018-01-24 11:08:26	0.0028171539306641
Edit Copy Delete	Umi Mahdiyah, S.Pd., M.Si	183 196 147 25	2018-01-24 11:08:27	0.0028510093688965
Edit Copy Delete	Umi Mahdiyah, S.Pd., M.Si	37 47 97 144	2018-01-24 11:08:28	0.0030210018157959
Edit Copy Delete	Umi Mahdiyah, S.Pd., M.Si	101 9 28 62 130 144	2018-01-24 11:08:30	0.002953052520752
Edit Copy Delete	Umi Mahdiyah, S.Pd., M.Si	95 186 130 144 121 103	2018-01-24 11:08:31	0.0027561187744141

Gambar 9. Pengujian Kecepatan Proses Elgamal (database)

Pengujian ini adalah pengujian kecepatan proses elagamal untuk itu pada database tabel “messages” ditambahkan field “kecepatan” untuk menampung nilai kecepatan prosesnya. Pada pengujian ini dapat ditarik kesimpulan bahwa plainteks yang sama tidak menghasilkan kecapatan yang sama karena chiperteks yang dihasilkan dari plainteks berbeda dan juga jumlah karakter plainteks yang banyak juga tidak berati kecepatannya semakin melambat karena semua kembali kepada chiperteks yang dihasilkan.

3.2.3 Pengujian Aplikasi Dengan Teknik SQL Injection (bypass login)

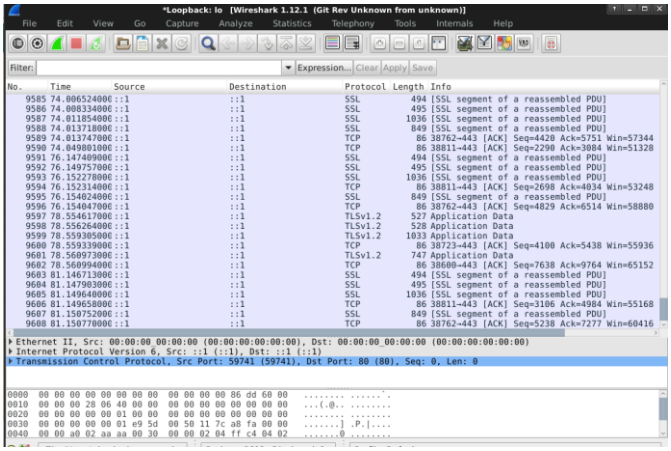


Gambar 10. Pengujian SQL Injection (bypass login)

Pengujian ini adalah pengujian keamanan form login dari teknik sql injection. Bisa dilihat aplikasi tidak bisa dibypass dengan query bypass login yang kebanyakan attacker gunakan.

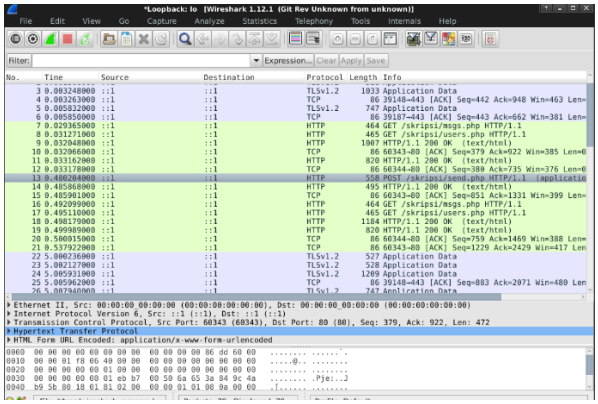
3.2.4 Pengujian Aplikasi Dengan Teknik Sniffing Menggunakan Tool Wireshark

Gambar 11. Pengujian Sniffing Dengan (dengan SSL)

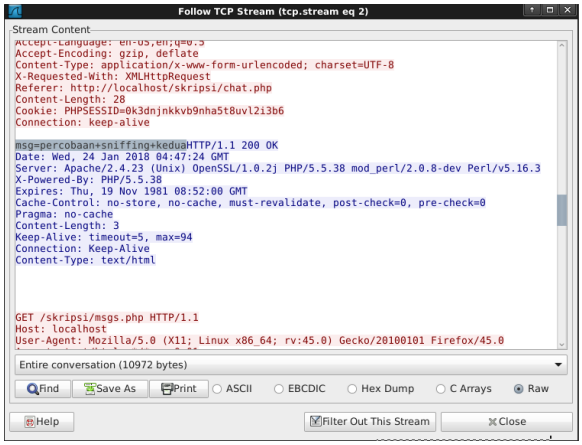


Gambar 12. Sniffing Aplikasi Group Chat(Dengan SSL)

Gambar 13. Pengujian Sniffing (tanpa SSL)



Gambar 14. Aplikasi Wireshark Melakukan Sniffing (tanpa SSL)



Gambar 15. Informasi Paket Yang Di Tangkap

Pengujian ini adalah pengujian aplikasi dengan teknik sniffing. Dalam pengujian ini dibuat jaringan lokal dimana skenarionya laptop Heru akan melakukan sniffing dengan tool wireshark untuk membaca pesan yang dikirimkan Alim pada aplikasi group chat. Pada Gambar 12 adalah contoh hasil sniffing dengan wireshark jika Alim menggunakan aplikasi group chat dengan protocol SSL dimana tidak ada packet yang dapat dibaca informasinya, hal itu disebabkan karena informasi packetnya telah dienkripsi sebelum melintas pada jaringan. Berbeda dengan Gambar 13, 14 dan 15 yang tidak menggunakan protokol SSL, informasi yang melintas bisa dengan mudah dibaca. Pada Gambar 13 Alim mengirimkan pesan "Percobaan sniffing kedua" dan pada Gambar 15 aplikasi wireshark menangkap informasi paket yang melintas di jaringan dan didapat informasi pesan yang dikirimkan Alim. Dari pengujian ini dapat disimpulkan penggunaan protokol SSL bisa melindungi pengguna dari teknik sniffing pada jaringan.

4. SIMPULAN

Setelah melalui beberapa tahapan dalam menyelesaikan Aplikasi Group Chat didapatkan kesimpulan sebagai berikut :.

4.2 Dihasilkan Aplikasi Group Chat yang mampu menerapkan algoritma kriptografi Elgamal dalam aplikasi Group Chat dengan cara menerapkan algoritma elgamal pada proses menginputkan pesan ke database dan menampilkan pesan dari database ke interface aplikasi.

4.3 Dan untuk membangun aplikasi Group Chat yang aman selain menggunakan algoritma kriptografi elgamal juga diperlukan penerapan protocol SSL pada aplikasi group chat.

5. SARAN

Pada penelitian ini tentu masih terdapat kekurangan yang dapat disempurnakan lagi pada pengembangan sistem berikutnya. Beberapa saran yang dapat dipergunakan diantaranya :

5.2 Aplikasi Group Chat ini perlu ditambah menu pengiriman berupa gambar, file dan emoticon.

5.3 Aplikasi perlu dirubah script jquerynya agar dapat dijalankan secara online.

5.4 Aplikasi perlu ditambahi fitur private chat sehingga dapat melakukan komunikasi dengan member lain satu per satu.

DAFTAR PUSTAKA

[1] Gupta, Anshul. 2013. A Research Study on Packet Sniffing Tool TCPDUMP, http://www.ijccts.org/books_pdf_dwd/A%20Research%20Study%20on%20Packet%20Sniffing%20Tool%20%20TCPDUMP.pdf), diakses pada tanggal 25 Mei 2017.

[2] A,Taufan,Yudhistira., Idris Winarno., Kholid Fathoni. Enkripsi Email Dengan Menggunakan Metode Elgamal Pada Perangkat Mobile. http://repo.pens.ac.id/1228/1/MAKALAH.pdf diakses pada tanggal 18 April 2016.

[3] Massandy, D.T. 2009. Algoritma Elgamal Dalam Pengamanan Pesan Rahasia. http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2009-2010/Makalah0910/MakalahStrukdis0910-056.pdf diakses pada tanggal 2 September 2017

[4] Sari, D.R. 2007. Keamanan SSL dalam Serangan Internet. http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah2/Makalah-045.pdf diakses pada tanggal 2 september 2017