ARTIKEL

PENERAPAN ALGORITMA ELGAMAL DALAM PEMBUATAN APLIKASI KONSULTASI PERWALIAN DI UNIVERSITAS NUSANTARA PGRI KEDIRI

Oleh:

Heru Aditya

13.1.03.02.0334

Dibimbing oleh :

1. **Intan Nur Farida, M.Kom**
2. **Risky Aswi Ramadhani, M. Kom**

PROGRAM STUDI

FAKULTAS

UNIVERSITAS NUSANTARA PGRI KEDIRI

TAHUN

2018

SURAT PERNYATAAN
ARTIKEL SKRIPSI TAHUN 2018

Yang bertanda tangan di bawah ini:

Nama Lengkap	:	Heru Aditya
NPM	:	13.1.03.02.0334
Telepun/HP	:	085730699729
Alamat Surel (Email)	:	aytidaureh@gmail.com
Judul Artikel	:	Penerapan Algoritma Elgamal Dalam Pembuatan Aplikasi Konsultasi Perwalian di Universitas Nusantara PGRI Kediri
Fakultas – Program Studi	:	Teknik – Teknik Informatika
Nama Perguruan Tinggi	:	Universitas Nusantara PGRI Kediri
Alamat Perguruan Tinggi	:	Jl. K.H. Ahmad Dahlan No. 76 Kota Kediri

Dengan ini menyatakan bahwa :

a. artikel yang saya tulis merupakan karya saya pribadi (bersama tim penulis) dan bebas plagiarisme;
b. artikel telah diteliti dan disetujui untuk diterbitkan oleh Dosen Pembimbing I dan II.

Demikian surat pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari ditemukan ketidaksesuaian data dengan pernyataan ini dan atau ada tuntutan dari pihak lain, saya bersedia bertanggungjawab dan diproses sesuai dengan ketentuan yang berlaku.

Mengetahui		Kediri , 5 Februari 2018
Pembimbing I	Pembimbing II	Penulis,
Intan Nur Farida, M.Kom NIDN. 0704108701	Risky Aswi Ramadhani, M.Kom NIDN. 0708049001	Heru Aditya NPM. 13.1.03.02.0334

PENERAPAN ALGORITMA ELGAMAL DALAM PEMBUATAN APLIKASI KONSULTASI PERWALIAN DI UNIVERSITAS NUSANTARA PGRI KEDIRI

Heru Aditya
13.1.03.02.0334
Fakultas Teknik – Program Studi Teknik Informatika
aytidaureh@gmail.com
Intan Nur Farida, M.Kom dan Risky Aswi Ramadhani, M. Kom
UNIVERSITAS NUSANTARA PGRI KEDIRI

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. Perwalian merupakan proses komunikasi yang dilakukan antara mahasiswa dan dosen wali. Chatting merupakan salah satu pilihan mahasiswa dalam melakukan konsultasi perwalian atau berkomunikasi dengan dosen wali.

Tujuan yang hendak ingin dicapai adalah membuat sebuah aplikasi konsultasi perwalian berupa aplikasi chatting dengan menerapkan algoritma kriptografi elgamal pada pesannya.

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. Sedangkan untuk pendekatan menggunakan pendekatan kuantitatif. Jenis pendekatan kuantitatif yang dipilih adalah noneksperimental berupa deskriptif.

Dari penelitian ini telah di hasilkan Aplikasi Konsultasi yaitu aplikasi konsultasi berupa aplikasi chatting. Aplikasi ini dibuat dengan menggunakan bahasa php,script jquery,dan database mysql. Aplikasi ini menerapkan algoritma kriptografi elgamal dalam proses mengenkripsi pesan yang dikirim ke database.

Berdasarkan hasil simpulan direkomendasikan : (1) Aplikasi Konsultasi 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: Aplikasi Konsultasi, Algoritma Kriptografi, Algoritma Elgamal, Aplikasi Chat, Chatting

I. LATAR BELAKANG

Seiring dengan pesatnya perkembangan jaman dan majunya teknologi saat ini membawa pengaruh besar pada aspek kehidupan manusia, salah satu contohnya adalah dalam hal komunikasi. Hal ini diperkuat dengan survei yang dilakukan APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) pada tahun 2016 yang menyatakan bahwa jumlah pengguna internet di Indonesia mencapai 51,8 % atau lebih dari setengah penduduk Indonesia. Berbagai macam penunjang komunikasi telah bermunculan seperti telepon genggam sampai internet sehingga kita dapat dengan mudah berkomunikasi dengan orang lain.

Perwalian merupakan proses komunikasi yang dilakukan antara mahasiswa dan dosen wali. Perwalian bertujuan untuk membantu mencarikan solusi bagi mahasiswa yang memiliki masalah dalam proses perkuliahannya. Chatting merupakan salah satu pilihan mahasiswa dalam melakukan perwalian atau berkomunikasi dengan dosen wali. Isi dari percakapan dalam proses perwalian bersifat rahasia sehingga diperlukan keamanan untuk melindungi isi percakapan tersebut. Tak sedikit orang yang berbuat curang untuk mencari tahu isi percakapan tersebut. Salah satunya dengan melakukan sql injection.

Melihat berbahayanya dampak dari sql injection maka dari itu diperlukan algoritma kriptografi. Salah satu algoritma kriptografi itu adalah algoritma ElGamal. Elgamal akan melindungi pesan yang ada di database dari sql injection. ElGamal ini akan di letakkan di tengah-tengah pengiriman pesan. Jadi sebelum pesan terkirim ke penerima, ElGamal akan mengenkripsi pesan tersebut sehingga yang akan terbaca di database bukan pesan murni melainkan pesan yang sudah di Enkripsi. Jika diterapkan pada aplikasi chatting, akan sangat membantu dalam menjaga kerahasian sebuah pesan karena algoritma ini mempunyai kelebihan pada enkripsi. “Karena untuk plainteks yang sama, algoritma ini memberikan cipherteks yang berbeda”.(Anshori.F. dkk., 2014:2).

Berdasarkan latar belakang masalah tersebut diatas, maka dibuatlah penulisan skripsi yang berjudul “Penerapan Algoritma Elgamal Dalam Pembuatan Aplikasi Konsultasi Perwalian Di Universitas Nusantara PGRI Kediri”.

II. METODE

A. Algoritma 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 .(Massandy, D.T, 2009)

B. SSL (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 . (Sari, D.R. 2007)

III. HASIL DAN KESIMPULAN

A. HASIL

Gambar 1. Tampilan Awal Aplikasi Konsultasi

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

Gambar 2. Halaman Login

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”.

Gambar 3. Tampilan Chats

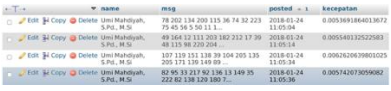
Pada tampilan chats terdapat percakapan dari dosen dan mahasiswa dan juga form input pesan yang siap disamarkan dengan proses enkripsi elgamal.

Percakapan yang tampil diambil dari database “chatting” tabel “messages” dan didekripsi menjadi plainteks.

Gambar 4. Tampilan Users

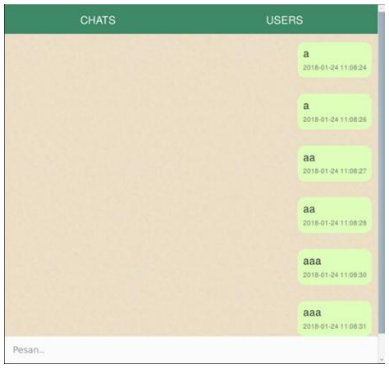
Tampilan users menampilkan daftar member siapa saja yang online yang diambil dari database “chatters”. Dan juga terdapat button Logout yang berfungsi untuk keluar atau offline dari aplikasi dan button Change Password yang akan mengantarkan kita ke tampilan Change Password.

Gambar 5. Pengujian Aplikasi Dengan Plainteks Sama (interface)

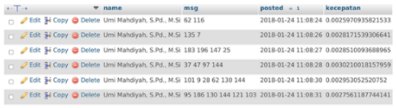


Gambar 6. Pengujian Aplikasi Dengan Plainteks Sama (database)

Pengujian pertama yaitu pengujian dengan plainteks yang sama yang di tunjukan pada Gambar 5 dan Gambar 6. Pada Gambar 5 terlihat plainteks yang ditampilkan sama, tapi berbeda dengan hasil enkripsi yang dihasilkan berbeda bisa dilihat pada Gambar 6 pada field “msg”.



Gambar 7. Pengujian Kecepatan Proses Elgamal (interface)



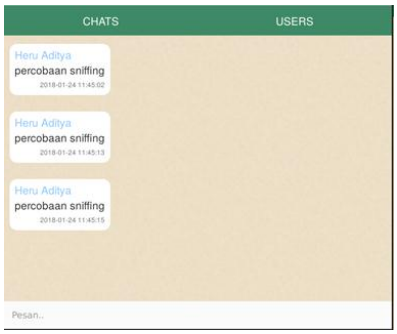
Gambar 8. Pengujian Kecepatan Proses Elgamal (database)

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

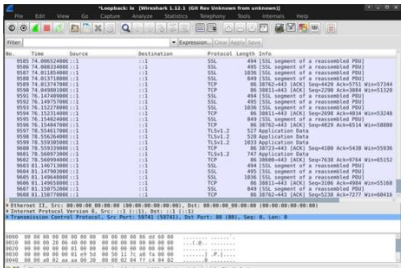
kesimpulan bahwa plainteks yang sama tidak menghasilkan kecapatan yang sama karena chiperteks yang dihasilkan dari plainteks berbeda dan juga jumlah karakter plainteks yang banyak juga tidak berati kecepatannya semakin melambat karena semua kembali kepada chiperteks yang dihasilkan.

Gambar 9. Pengujian SQL Injection (bypass login)

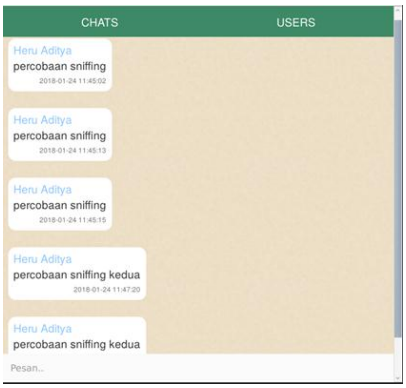
Pengujian ini adalah pengujian keamanan form login dari teknik sql injection. Bisa dilihat aplikasi tidak bisa dibypass dengan query bypass login yang kebanyakan attacker gunakan.



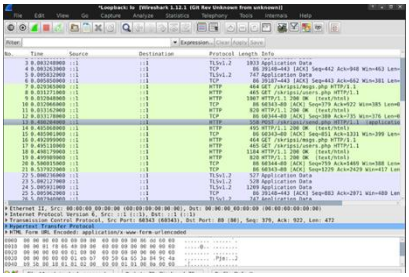
Gambar 10. Pengujian Sniffing Dengan (dengan SSL)



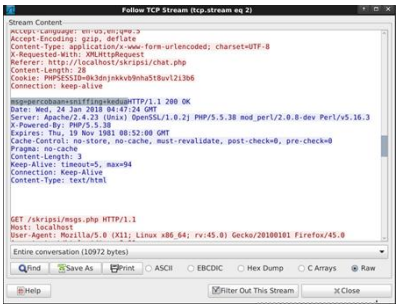
Gambar 11. Sniffing Aplikasi Group Chat(Dengan SSL)



Gambar 12. Pengujian Sniffing (tanpa SSL)



Gambar 13. Aplikasi Wireshark Melakukan Sniffing (tanpa SSL)



Gambar 14. 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 11 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 12, 13 dan 14 yang tidak menggunakan protokol SSL, informasi yang melintas bisa dengan mudah dibaca. Pada Gambar 12 Alim mengirimkan pesan "Percobaan sniffing kedua" dan pada Gambar 14 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

B. KESIMPULAN

Setelah melalui beberapa tahapan dalam menyelesaikan Aplikasi Konsultasi Perwalian.

1. Dihasilkan Aplikasi Konsultasi Perwalian yang mampu menerapkan algoritma kriptografi Elgamal dalam aplikasi konsultasi perwalian dengan cara menerapkan algoritma elgamal pada proses menginputkan pesan ke database dan menampilkan pesan dari database ke interface aplikasi.
2. Untuk membangun aplikasi konsultasi perwalian yang aman selain menggunakan algoritma kriptografi elgamal juga diperlukan penerapan protocol SSL pada aplikasi konsultasi perwalian.

IV. DAFTAR PUSTAKA

Al-Anshori, Faqihuddin., Aribowo, Eko. 2014. *Implementasi Algoritma Kriptografi Kunci Publik Elgamal Untuk Proses Enkripsi Dan Dekripsi Guna Pengamanan File*

Data,(Online),tersedia:http://download.portalgaruda.org/article.php?article=374916&val=5555&title=IMPLEMENTASI%20ALGORITMA%20KRIPTOGRAFI%20KUNCI%20PUBLIK%20ELGAMAL%20UNTUK%20PROSES%20ENKRIPSI%20DAN%20DEKRIPSI%20GUNA%20PENGAMANAN%20FILE%20DATA), diunduh 25 Mei 2017.

Massandy, D.T. 2009. *Algoritma Elgamal Dalam Pengamanan Pesan Rahasia*, (Online), tersedia : http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2009-2010/Makalah0910/MakalahStrukdis0910-056.pdf), diunduh 2 September 2017.

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