KRIPTOGRAFI MMS PADA APLIKASI JAVA MENGGUNAKAN ALGORITMA AES
MMS CRYPTOGRAPHY AT JAVA APPLICATION USING ALGORITHM AES

David Ruslim[1], -[2]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Perkembangan teknologi telekomunikasi pada saat ini telah mengubah cara masyarakat dalam berkomunikasi. Pada zaman sekarang ini, telah banyak masyarakat yang melakukan komunikasi dengan menggunakan Mobile Seluler salah satunya adalah komunikasi dengan menggunakan sistem Messaging Service. Messaging Service berkembang dari SMS menjadi EMS dan sekarang MMS. SMS hanya mampu mengirimkan pesan berupa teks, EMS sudah mendukung pengiriman gambar, sedangkan MMS mendukung pengiriman pesan berupa teks, gambar, suara, dan video. Dalam pengiriman pesan yang dilakukan si pengguna Mobile Seluler untuk sekarang ini, penulis berpendapat bahwa masih kurangnya keamanan akan pengiriman pesan ataupun data informasi yang akan dikirimkan, kemungkinan penyadapan pesan atau data informasi cukup relatif besar. Berdasarkan perkembangan dalam messaging service tersebut maka dalam tugas akhir ini penulis membangun sebuah sistem keamanan pada messaging service. Sistem keamanan yang dibuat adalah Kriptografi pesan atau data informasi yang akan dikirimkan, untuk tugas akhir ini penulis mengkhususkan sistem yang di Kriptografikan yaitu Multimedia Message Service (MMS). Sistem mengenkripsikan pesan atau data informasi berupa MMS pengirim kemudian diterima oleh penerima setelah itu penerima melakukan dekripsi pada MMS yang telah dikirim. Algoritma kriptografi yang digunakan adalah AES (Advanced Encryption Standard) yaitu algoritma yang dikembangkan oleh Rijndael.

Dilihat dari analisa yang dilakukan diketahui bahwa ukuran besar MMS sangat mempengaruhi proses enkripsi dan dekripsi MMS. Semakin besar ukuran MMS semakin lama waktu proses.

Kata Kunci : mobile seluler, Multimedia Message Service (MMS), kriptografi , enkripsi, dekripsi

Abstract

Development in telecomunication technology at the moment have altered the way society in communicating. At this present day, have a lot of society doing communications by using Mobile Seluler one of them is communications by using system of Messaging Service. Messaging Service expand from SMS become EMS and now MMS. SMS only able to deliver message in the form of text, EMS have supported delivery image, while MMS support delivery order in the form of text, image, voice, and video. In message delivery conducted the consumer of Mobile Seluler to this time, writer have a notion that still the lack of delivery security in delivery message or data information to be delivered, possibility of tapped message or data information enough big relative.

Pursuant to growth in The Messaging Service hence in this final task writer try to develop a security system at messaging service. Security system to be made is cryptography message or data information to be delivered, for the this final task writer major system to cryptography that is Multimedia Message Service (MMS). System will be encryption of message or data information in the form of MMS sender, then be accepted by receiver afterwards the receiver conduct decription MMS which have been sent. Algorithm cryptography use is AES (Advanced Encryption Standard) that is algorithm developed by Rijndael.

Based on the analysis taken, it is proven that size MMS have take effect for encryption and decryption process of MMS. More bigger size of MMS can made a long time for process.

Keywords : mobile seluler, Multimedia Message Service (MMS), kriptografi , encryption, decryption

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dewasa ini perkembangan teknologi komputer dan teknologi telekomunikasi pada saat ini mengubah cara masyarakat berkomunikasi. Dulu, komunikasi jarak jauh masih dilakukan dengan cara konvensional, yaitu dengan cara mengirim surat. Sekarang adanya internet dan teknologi komunikasi yang sangat pesat, komunikasi jarak jauh bisa dilakukan dengan cara saling mengirim email atau menggunakan media messaging service (SMS, MMS). Untuk teknologi dalam jenis mobile seluler seperti teknologi SMS misalnya, sekarang ini telah banyak digunakan untuk melakukan pertukaran informasi-informasi yang biasa sampai informasi yang penting dari pengguna mobile seluler tersebut. Kemudian berkembang teknologi MMS yagn mulai digunakan sebagai alat pemasaran produk karena MMS tidak hanya dapat mengirimkan pesan teks tetapi juga mendukung pengiriman pesan berupa gambar, video, audio dan kombinasinya.

Namun tidak semua perkembangan teknologi komunikasi ini memberikan dampak yang menguntungkan bagi dunia komunikasi. Penyadapan data merupakan hal yang ditakuti oleh pengguna jaringan komunikasi pada saat ini. Masalah keamanan dan kerahasian data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Apabila data atau informasi yang akan dikirimkan tidak diberikan keamanan. Tentu saja data atau informasi yang sangat penting tersebut dapat dilihat atau dibajak oleh orang yang tidak berwenang. Sebab kalau hal ini sampai terjadi kemungkinan data atau informasi yang dikirimkan akan rusak bahkan bisa hilang yang akan menimbulkan kerugian-kerugian yang bersifat material atau kerugian yang lain. Apalagi, apabila pemilik data atau informasi adalah pihak militer atau pemerintah, keamanan dalam pertukaran informasi menjadi sangat penting karena data yang mereka kirim kebanyakan adalah data-data rahasia yang tidak boleh diketahui oleh publik.

Dalam tugas akhir ini penyusun lebih memfokuskan sistem keamanan pada messaging service yang berupa kriptografi multimedia message service (MMS). Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Kriptografi merupakan kajian ilmu dan seni untuk menjaga pesan atau data informasi agar data atau informasi tersebut aman. Sistem kriptografi MMS yang akan dibuat ini nantinya akan memberikan keamanan bagi pengirim dan penerima karena dalam sistem ini pengirim akan melakukan enkripsi pada data atau informasi yang akan dikirimkan dalam MMS setelah itu penerima akan melakukan dekripsi pada MMS yang telah dikirim kemudian penerima akan mendapatkan data atau informasi yang telah dikirimkan pengirim.

1.2 Perumusan Masalah

Pada zaman sekarang ini kebanyakan masyarakat melakukan komunikasi dengan mobile seluler, mereka mengirimkan data atau informasi yang sangat penting atau pribadi dengan sembarang dan tidak memikirkan tingkat keamanan yang ada. Sedangkan sekarang ini telah banyaknya penyadapan-penyadapan yang dilakukan secara langsung maupun tidak langsung.

Contohnya: Sesorang mengirimkan data perusahaannya yang sangat penting dengan menggunakan MMS kepada rekannya yang berada di luar daerah, apabila tidak diikuti sistem keamanan yang baik kemungkinan data tersebut dapat dilihat oleh orang lain yang sedang menggunakan aplikasi java si penerima data. Apabila si pengirim menggunakan jasa kurir kirim kemungkinan data yang dikirim tidak langsung sampai, karena menggunakan waktu yang cukup lama dan pengirim juga akan mengeluarkan biaya menjadi lebih besar.

Berdasarkan permasalahan di atas, penulis memiliki inisiatif untuk membangun suatu sistem keamanan komunikasi berupa kriptografi MMS dimana si pengguna aplikasi java dapat mengirimkan data informasi penting mereka dengan cepat, aman, dan tidak mengeluarkan biaya yang cukup besar.

1.3 Tujuan Pembahasan

Tujuan yang ingin dicapai dari penyusunan tugas akhir ini adalah :

1. Membangun suatu sistem keamanan dalam pengiriman pesan dengan menggunakan MMS.
2. Menganalisa performansi (Waktu yang dibutuhkan untuk mengenkripsi dan dekripsi MMS) dari sistem yang dibangun.

1.4 Batasan Masalah

Dalam pembangunan aplikasi ini dibatasi beberapa hal yaitu:

1. Tidak mengatasi kesalahan yang dilakukan operator seluler.
2. Hanya menggunakan jenis mobile seluler yang dapat menggunakan Java.
3. Hanya menangani enkripsi dan dekripsi teks dan image saja.

1.5 Metodologi Penyelesaian Masalah

Pengerjaan tugas akhir ini menggunakan metodologi :

- Studi Literatur

  Bertujuan mempelajari dasar teori dan literatur-literatur mengenai MMS, algoritma AES.
- Pengumpulan Data

  Bertujuan untuk mengumpulkan informasi dan data-data yang berhubungan dengan pembangunan perangkat lunak.
- Studi Analisa dan Pengembangan Sistem

  Bertujuan menganalisa kebutuhan perangkat lunak dan melakukan perancangan dan desain perangkat lunak.
- Implementasi dan uji coba

  Bertujuan mengimplementasikan perancangan dan desain yang telah dibuat, kemudian melakukan uji coba terhadap perangkat lunak yang telah dibuat.
- Analisa Performansi

  Bertujuan melakukan uji performansi perangkat lunak.
- Kesimpulan dan Saran

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Berisi latar belakang, perumusan masalah, tujuan pembahasan, batasan masalah, metodologi penyelesaian masalah dan sistematika penulisan.

BAB II LANDASAN TEORI

Berisi penjelasan umum tentang landasan teori yang berkaitan dengan penyusunan tugas akhir.

BAB III ANALISA DAN DESAIN

Berisi analisis sistem yang akan dikembangkan mencakup analisa kebutuhan sistem, perancangan dan desain sistem, sehingga dapat dipahami dengan mudah.

BAB IV IMPLEMENTASI DAN EVALUASI

Mengimplementasikan sistem dengan memperhatikan analisa kebutuhan sistem, perancangan dan desain sistem, serta melakukan pengujian fungsional dan performansi sistem.

BAB V KESIMPULAN DAN SARAN

Diuraikan kesimpulan dan saran yang didapat dari hasil pengembangan sistem.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Beberapa kesimpulan yang dapat diambil adalah sebagai berikut :

1. Dalam tugas akhir ini penulis berhasil membuat sistem yang dapat melakukan proses enkripsi dan dekripsi pada MMS.
2. Sistem memberikan keamanan kepada user pada saat akan mengirimkan MMS yang penting.
3. Dalam waktu proses enkripsi dan dekripsi yang sangat penting dalam sistem yaitu besar MMS yang dibuat.
4. Ukuran besar MMS sangat mempengaruhi proses. Semakin besar ukuran MMS semakin lama waktu proses.
5. Besar Image lebih berpengaruh daripada banyaknya teks dalam proses enkripsi dan dekripsi.
6. Untuk proses enkripsi dan dekripsi dengan besar >100 KB waktu prosesnya melewati dari waktu proses standar.
7. Diketahui pada pengujian proses enkripsi dengan besar MMS >117 KB proses tidak dapat dilakukan.
8. Proses Enkripsi dan Dekripsi yang baik adalah apabila waktu respon enkripsi/dekripsi lebih kecil daripada waktu standar enkripsi/dekripsi.

5.2 Saran

Beberapa saran untuk pengembangan sistem selanjutnya adalah sebagai berikut :

1. Dalam pengembangan sistem ini berikutnya sebaiknya dapat melakukan proses pengiriman.
2. Dalam pengiriman MMS operator seluler sebaiknya menerima penanganan MMS yang terenkripsi.

3. Dalam melakukan proses enkripsi dan dekripsi sebaik mungkin bisa lebih cepat dari sistem yang dibuat.
4. Sistem tidak hanya melakukan proses enkripsi dan dekripsi teks dan image saja, sistem dapat melakukan proses untuk suara dan video.
5. Sistem yang dibuat dapat digunakan oleh berbagai emulator dan mobile seluler yang ada.

DAFTAR PUSTAKA

[1] Abdurohman, Maman. Analisa Performansi Algoritma Kriptografi RC6. ITB. 2002

[2] AW, Wihartantyo. Advanced Encryption Standard, Algoritma Rjindael. ITB. 2004.

[3] Mobilecomm Lab. Modul MMS Short Course. STT Telkom. 2004.

[4] OMA. Multimedia Messaging Service Encapsulation Protocol version 1.1. 2002

[5] OMA. Multimedia Messaging Service Client Transactions version 1.1. 2002

[6] Heriyanti, Tedi. Pengenalan Kriptografi. 1999

[7] RH, Patira. Algoritma dan Implementasi Advanced Encryption Standard. ITB. 2004.

[8] Wicaksono, Ady. Pemrograman Aplikasi Wireless dengan Java. Alex Media Komputindo. 2002.

[9] www.aes.crockatt.com

[10] www. java.sun.com

[11] www.java2s.com