PERANCANGAN SISTEM ENKRIPSI DATA SMS (SHORT MESSAGE SERVICE) PADA APLIKASI XMS (XECURE MESSAGE SERVICE)

Fx Laga Satya A P[1], R. Rumani[2], Indrarini D I.[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Salah satu bentuk komunikasi yang sering digunakan user adalah SMS (Short Message Service), dimana informasi yang dikirimkan berupa teks. Namun, SMS bukan merupakan pilihan terbaik untuk komunikasi yang aman. Kebanyakan user tidak menyadari betapa mudahnya mencuri isi sebuah pesan. Spesifikasi dan teknologi mendasar dari SMS masih banyak terdapat celah keamanan yang menyebabkan SMS bukan merupakan jalur aman untuk berkomunikasi

Tugas akhir ini mengusulkan sebuah konsep keamanan terhadap komunikasi SMS, dimana perancangan sistem enkripsi data SMS yang akan dibuat aplikasi disebut XMS (Xecure Message Service). Teknik enkripsi yang dibuat menggunakan algoritma AES dan algoritma RC4 sebagai pembanding. Pada aplikasi ini juga ditambahkan PIN untuk melakukan proses enkripsi ataupun dekripsi. Sistem tersebut selanjutnya diuji dengan menjalankan aplikasi yang telah dibuat untuk mengetahui performansinya.

Dari hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa perancangan aplikasi ini dapat bekerja dengan baik. Hal ini terlihat dari aplikasi XMS yang telah dibuat dapat mengenkripsi data SMS dan mengirimkannya dalam keadaan terenkripsi. Di sisi lain, data SMS yang diterima dapat didekripsi dan diketahui isi pesan sesungguhnya. Aplikasi XMS terbukti aman karena memenuhi aspek-aspek keamanan kriptografi. Tingkat keberhasilan enkripsi dan dekripsi pesan dengan algoritma AES adalah 100%. Tingkat keberhasilan enkripsi dan dekripsi dengan algortima RC4 adalah 10% - 40%, karena mengalami kendala pada telepon seluler dalam mendefinisikan karakter hasil enkripsi.

Kata Kunci : Short Message Service, Xecure Message Service, AES Algorithm,RC4 Algorithm, PIN.

Abstract

One of communication which is often to be used by users is SMS (Short Message Service), which the information is sent is text. But SMS is not the best choice to communicate safely. Most of users do not attend how very easy to steal the contents of message. Specification and base technology of SMS still have slots of security that cause SMS is not the secure way to communication.

This final project proposes a concept of security for SMS communication. That is encryption system SMS data planning which will be built the application is called XMS (Xecure Message Service). Encryption technique that is built is using AES algorithm and RC4 algorithm as the comparison. In this application is added PIN too for processing the encryption or decryption. Furthermore the system is tested with start the application which has been built to know the performances.

From the research which have been done, can be concluded that this application planning works properly. This thing is seen from the XMS application which has been built can encrypt the SMS data and send it in encrypted condition. In the other side, the SMS data which is received can be decrypted and can be known the real message. XMS application is secure because it can fulfill aspects of cryptograph security. The success encryption and decryption messages with AES algorithm is 100%. The success encryption and decryption messages with RC4 algorithm is between 10% - 40%, because it has obstacle at mobile phone in identification encrypted characters.

Keywords : Short Message Service, Xecure Message Service, AES Algorithm,RC4 Algorithm, PIN.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Salah satu layanan dalam dunia telekomunikasi bergerak adalah *Short Message Service* atau lebih dikenal dengan sebutan SMS. SMS adalah salah satu tipe *Instant Messaging* (IM) yang memungkinkan pelanggan untuk bertukar pesan singkat kapanpun, walaupun *user* sedang melakukan *call* data/suara.

Dari awal tebentuknya komunikasi bergerak hingga perkembangan teknologi saat ini, SMS masih menjadi pilihan bagi pelanggan dalam menyampaikan pesan singkat kepada pelanggan lain. Hal ini disebabkan karena penggunaan SMS lebih mudah dan umum digunakan oleh pelanggan dari semua kalangan.

Dalam kehidupan sehari-hari SMS lebih sering digunakan oleh pelanggan daripada layanan yang lain. Untuk permintaan pelanggan tertentu, dalam proses sebelum SMS dikirim diperlukan adanya proteksi pada SMS. Sehingga pesan yang dikirim oleh pelanggan tertentu tidak dapat dibuka oleh sembarang pelanggan.

1.2 Tujuan Penelitian

Tujuan penelitian dari Tugas Akhir ini adalah membuat suatu sistem pengamanan data SMS yang berupa text. Hal ini dapat dilakukan dengan menjalankan proses enkripsi data text tersebut, dengan menggunakan perangkat telepon seluler MC-35 dan komputer yang akan dibuat antarmuka dalam bentuk *software Xecure Message Service* (XMS).

1.3 Perumusan Masalah

Dalam tugas akhir ini dibahas mengenai perancangan sistem pengamanan data SMS dengan membuat software *Xecure Message Service*. Sistem tersebut memiliki bagian-bagian utama yaitu: telepon seluler MC-35,

komputer, dan software XMS. Permasalahan yang menjadi objek dalam penelitian tugas akhir ini adalah:

1. Mengkoneksikan bagian-bagian utama tersebut menjadi sebuah sistem yang dapat berfungsi sesuai dengan tujuan penelitian di atas.
2. Pemrograman menggunakan Visual Basic 6.0.
3. Perfomansi yang dihasilkan oleh sistem tersebut yang meliputi: enkripsi data SMS, perfomansi pengiriman SMS, dan dekripsi data SMS.

1.4 Batasan Masalah

1. Aplikasi dilakukan pada jalur komunikasi SMS.
2. Perangkat yang digunakan adalah *Personal Computer* dan telepon seluler yang mendukung seperti Siemens MC35.
3. Algoritma yang digunakan adalah algoritma AES dan RC4.
4. *Software* yang digunakan untuk pembuatan XMS adalah Visual Basic 6.0.
5. Aplikasi dilakukan pada jaringan GSM.
6. Asumsi hal-hal yang berkaitan dengan *human error* diabaikan.

1.5 Metode Penelitian

Metode yang akan digunakan dalam tugas akhir ini adalah sebagai berikut:

a. Tahap studi literatur

   Melakukan studi literature mengenai konsep SMS dan aplikasinya.

b. Tahap perancangan

   Melakukan perancangan dan pemodelan pada sistem yang akan diuji. Hal ini berkaitan dengan relevansinya di lapangan dan kemungkinannya untuk disimulasikan.

c. Tahap simulasi dan pengumpulan data

   Mengumpulkan data-data dari parameter yang telah ditentukan dari hasil pengujian pada implementasi jaringan.

d. Tahap analisis dan penarikan kesimpulan

   Melakukan analisis dari data yang telah didapatkan dari hasil pengujian dan simulasi.

1.6 Sistematika Penulisan

Tugas Akhir ini disusun berdasarkan sistematika sebagai berikut :

BAB 1 : Pendahuluan

Pada bab ini dibahas mengenai latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan masalah, metodologi penelitian, hipotesis, dan sistematika penulisan tugas akhir.

BAB 2 : Dasar Teori

Pada bab ini dipaparkan berbagai dasar teori yang mendukung dan mendasari penulisan tugas akhir ini.

BAB 3 : Perancangan Sistem dan Implementasi

Pada bab ini dijelaskan mengenai proses perancangan aplikasi proteksi pada jalur komunikasi SMS.

BAB 4 : Pengujian Sistem dan Analisis

Pada bab ini dilakukan pengujian sistem dan analisis hasil yang diperoleh dari tahap perancangan dan aplikasi.

BAB 5 : Kesimpulan dan Saran

Pada bab ini diberikan kesimpulan mengenai permasalahan yang dibahas berdasarkan serangkaian penelitian yang dilakukan. Selain itu, pada bab ini juga akan diberikan saran untuk pengembangan selanjutnya.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari perancangan sistem enkripsi SMS pada aplikasi XMS yang dilakukan pada tugas akhir ini, maka dapat diambil kesimpulan sebagai berikut:

1. Aplikasi XMS berfungsi dengan baik, terbukti dapat memudahkan *user* untuk melakukan enkripsi, pengiriman, dan dekripsi pesan.
2. Tingkat keberhasilan enkripsi dan dekripsi pesan menggunakan algoritma AES adalah 100%.
3. Tingkat keberhasilan enkripsi dan dekripsi pesan menggunakan algoritma RC4 adalah 10% - 40%, karena mengalami kendala pada telepon seluler dalam mendefinisikan karakter hasil enkripsi.
4. Pada enkripsi algoritma AES, setiap penambahan jumlah 16 karakter pada teks asli akan terjadi penambahan sebanyak 64 bit karakter pada hasil enkripsi. Dan akan tetap setelah bit karakter mencapai jumlah 256 bit.
5. Aplikasi XMS terbukti meningkatkan keamanan dalam pertukaran informasi, terbukti dari hasil percobaan simulasi yang memenuhi aspek-aspek keamanan kriptografi yaitu aspek kerahasiaan, integritas data, autentikasi, dan menolak penyangkalan.

5.2 Saran

1. Untuk penelitian lebih lanjut dapat digunakan telepon seluler yang memiliki *Symbian OS* atau telepon seluler berbasis *Java*.
2. Untuk pembuatan aplikasi yang memiliki fitur lebih lengkap dapat digunakan program berbasis *Java*.

DAFTAR PUSTAKA

[1] A Brief Introduction to Secure SMS Messaging in MIDP FORUM NOKIA Version 1.0; September 23, 2003. Pdf

[2] Denis Pankratov, Dmitri Kramarenko. 2004. *SMS spoofing - Q&A with CCRC staff*. http://www.crime_research.org/interviews/sms-spoofing-intro. Didownload pada 29 Juli 2009.

[3] Job de Haas. 2001. Mobile security: SMS and WAP nada. http://www.itsec.gov.cn/web_portal/download.ppt. Didownload pada 3 Agustus 2009.

[4] John. Wiley. and. Sons., "MOBILE MESSAGING TECHNOLOGIES AND SERVICES SMS, EMS and MMS. 2ed.", Mar 2005. eBook-DDU. pdf

[5] http://www.asianlaws.org/hitlist.pdf. Didownload pada 29 Juli 2009.

[6] http://www.cs.huji.ac.il/~sans/students_lectures/GSM%20Attacks.ppt. Didownload pada 29 Juli 2009.

[7] http://www.microsoft.com/smsserver/techinfo/deployment/secessential.html. Didownload pada 29 Juli 2009.

[8] http://www.mynetsec.com/files/xms_manager/XMS_Manager_White_Paper.pdf. Didownload pada 3 Agustus 2009

[9] SMS Sequrity. http://www.odysseytec.com/solutions/sms_security.html. Didownload pada 29 Juli 2009.

[10] Sun Microsystem. 2003. *System Management Services Software: An Inside Look*. http://www.informit,com/articles.html. Didownload pada 3 Agustus 2009.