IMPLEMENTASI ALGORITMA RC4 UNTUK ENKRIPSI SMS PADA TELEPON SELULAR

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk mendapatkan gelar Ahli Madya
pada Jurusan Teknologi Informasi Program Studi Teknik Komputer

Oleh:

RANDY WISKA
BP. 05092006

PROGRAM STUDI TEKNIK KOMPUTER
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK UNIVERSITAS ANDALAS
PADANG

2009

ABSTRAKSI

Pada tugas akhir ini dibangun suatu perangkat lunak yang dapat berguna untuk meningkatkan keamanan pesan yang terjadi pada komunikasi melalui SMS. SMS merupakan suatu layanan yang diberikan oleh telepon selular kepada penggunanya untuk melakukan komunikasi melalui pengiriman pesan singkat dengan biaya yang murah. SMS sangatlah populer, selain dikarenakan biayanya yang murah, pesan yang dikirimkan dapat diterima oleh penerima dengan baik dan cepat. Namun komunikasi melalui media SMS ini bukanlah komunikasi *point-to-point*, pesan yang dikirimkan melalui media SMS tidak langsung sampai pada tujuan, melainkan melalui jaringan SMS. Pada jaringan SMS tersebut, keamanan pesan sangatlah terancam untuk dibaca oleh orang yang tidak bertanggung jawab. Perangkat yang dibangun meningkatkan keamanan pesan dengan melakukan enkripsi terhadap pesan yang dikirimkan.

Perangkat lunak yang dibangun menggunakan algoritma RC4 untuk melakukan enkripsi SMS agar keamanan pesan dapat ditingkatkan. Algoritma RC4 adalah suatu algoritma kunci *public* yang dikenal dengan kesederhanaannya. Untuk keamannya, algoritma RC4 mengutamakan prinsip *stream cipher*.

Perangkat lunak yang dibangun menggunakan teknologi J2ME yang dapat ditanamkan pada telepon selular. Berdasarkan pengujian perangkat lunak yang dilakukan pada telepon selular dapat dilihat bahwa perangkat lunak dapat berjalan dengan baik dan algoritma RC4 dapat diimplementasikan untuk enkripsi SMS pada telepon selular.

Kata Kunci: SMS, RC4, *stream cipher*, J2ME, enkripsi, dekripsi

BAB I

PENDAHULUAN

1.1 Latar Belakang

Telepon selular merupakan alat komunikasi yang sudah dipakai oleh sebagian besar orang didunia. Telepon selular menyediakan media komunikasi yang beragam dan salah satu diantaranya adalah media SMS (*short message service*). SMS merupakan suatu layanan yang memungkinkan pengguna telepon selular untuk mengirimkan pesan singkat kepada pengguna telepon selular lainnya dengan cepat dan dengan biaya yang kecil.

Layanan pengiriman SMS ini sangatlah standar dan tidak jarang para pengguna telepon selular menggunakan layanan SMS ini untuk mengirimkan suatu pesan yang penting dan rahasia, namun para pengguna layanan SMS tersebut sering kali tidak mengetahui bahwa jalur komunikasi SMS memiliki banyak sekali celah yang memungkinkan untuk terjadinya serangan pada pesan teks yang dikirim.

Untuk mengurangi resiko yang ditimbulkan dari celah – celah yang terdapat pada layanan SMS tersebut salah satu cara penanggulangannya adalah dengan menerapkan suatu algoritma kriptografi pada pesan yang dikirimkan. Dengan terenkripsinya pesan yang dikirim maka seseorang yang berhasil mencuri informasi pesan teks yang dikirim tersebut akan kesulitan untuk mengetahui isi dari pesan tersebut. Dengan kemajuan teknologi telepon selular, dimana bermunculan telepon selular yang memiliki memori yang cukup besar sehingga

memungkinkan untuk melakukan implementasi enkripsi pada SMS jadi kenyataan.

1.2 Rumusan Masalah

Rumusan masalah yang akan dibahas pada tugas akhir ini diantaranya :

1. Bagaimana mengimplementasikan algoritma RC4 pada telepon selular ?
2. Bagaimana bentuk aplikasi enkripsi dengan menggunakan algoritma RC4 yang diimplementasikan untuk enkripsi SMS ?

1.3 Tujuan

Tujuan yang akan dicapai dalam pelaksanaan tugas akhir ini diantaranya :

1. Memahami algoritma RC4 dengan melakukan implementasi pada telefon selular
2. Melakukan pengujian dari aplikasi yang telah dibangun

1.4 Batasan Masalah

Batasan yang akan diambil dalam tugas akhir adalah sebagai berikut :

1. Penanganan enkripsi akan dilakukan sewaktu pesan teks dikirimkan
2. Analisis keamanan tidak akan dibahas
3. Aplikasi yang dibangun merupakan aplikasi yang berdiri sendiri, akan terpisah dari aplikasi SMS standar yang dimiliki telepon seluler

BAB V

PENUTUP

Pada bab V ini akan diambil kesimpulan dari kegiatan-kegiatan yang telah dilakukan selama pengerjaan tugas akhir ini, selain itu terdapat saran-saran untuk pengembangan lebih lanjut yang dapat diberikan dari tugas akhir ini.

5.1 Kesimpulan

Kesimpulan yang didapat selama pengerjaan tugas akhir ini adalah sebagai berikut:

1. Sebuah perangkat lunak yang mengimplementasikan suatu algoritma kriptografi untuk enkripsi SMS telah berhasil dibangun. Perangkat lunak yang dibangun tersebut dapat melakukan pengiriman pesan dan penerimaan pesan terenkripsi tersebut dengan baik. Perangkat lunak tersebut menggunakan algoritma RC4 untuk enkripsi SMS. Perangkat lunak tersebut ditanamkan pada telepon selular dan dibangun dengan menggunakan bahasa pemrograman java.
2. Pengujian aplikasi yang telah dibangun dilakukan pada *handphone* Nokia 2630 dan Nokia 3120 classic berhasil dilakukan. Pengiriman pesan yang terenkripsi diuji pada handphone Nokia 2630 dan penerimaan pesan yang terenkripsi diuji cobakan pada handphone Nokia 3120 classic.
3. Algoritma RC4 merupakan algoritma kriptografi *stream cipher* yang sederhana dan mudah untuk diimplementasikan. Pada algoritma RC4 cipherteks berasal dari plainteks yang di-XOR-kan dengan *keystream* atau kunci yang dibangkitkan.

DAFTAR PUSTAKA

Arsyad, Arniaty. *Membuat SMS Server Sendiri.* http://hotcopensourcecode.blogspot.com/2008/11/mari-membuat-sms-server-sendiri-3.html .

Irawan. Java Mobile Untuk Orang Awam. Palembang : Maxikom, 2008.

Raharjo, Budi., Imam Heryanto., Arif Haryono. Mudah Belajar Java. Bandung : INFORMATIKA, 2007.

Rinaldi. Bahan Kuliah IF5054 Kriptografi : RC4 dan A5. ITB, 2008.

Wikipedia. *RC4*. http://en.wikipedia.org/wiki/RC4.