Aplikasi Enkripsi SMS Menggunakan Metode Blowfish

Galih Wahyu Prasetyo

***Abstract*—Pada proyek akhir ini akan dibangun suatu perangkat lunak yang berguna meningkatkan keamanan pesan SMS. Perangkat lunak yang dibangun ini meningkatkan keamanan pesan dengan melakukan enkripsi terhadap pesan yang akan dikirimkan menggunakan metode enkripsi Blowfish. Algoritma Blowfish adalah suatu algoritma enkripsi simetris yang berarti bahwa algoritma ini menggunakan kunci yang sama baik untuk melakukan proses enkripsi dan dekripsi. Aplikasi ini dibangun menggunakan J2ME karena J2ME dapat berjalan pada banyak platform dimana terdapat JVM.**

***Index Terms*—SMS, Enkripsi, Blowfish, J2ME**

I. Pendahuluan

Telepon seluler merupakan alat komunikasi yang umum dipakai oleh sebagian besar umat manusia di dunia. Telepon seluler juga menyediakan media komunikasi yang beragam, salah satunya adalah SMS. Penggunaan SMS menjadi popular di kalangan masyarakat karena dengan begitu mudahnya kita dapat saling bertukar informasi tanpa batasan jarak dan waktu. Celah keamanan terbesar pada komunikasi via SMS adalah pesan yang dikirimkan akan disimpan di SMSC (Short Message Service Center), yaitu tempat dimana SMS disimpan sebelum dikirim ke tujuan. Pesan yang sifatnya plaintext ini dapat disadap oleh siapa saja yang berhasil memiliki akses ke dalam SMSC. Akibatnya, informasi penting seperti password, nomer pin, dan lain-lain dapat dibaca oleh orang yang tidak berhak untuk mengetahuinya. Proyek akhir ini akan memberikan alternatif untuk menyelesaikan masalah ini. Dengan semakin majunya teknologi pada telepon seluler, implementasi suatu algoritma menjadi mungkin dilakukan. Macam-macam algoritma enkripsi antara lain : DES, IDEA, AES, Blowfish dan masih banyak lagi. Algoritma Blowfish digunakan dalam pembuatan proyek akhir ini. Algoritma ini dirancang untuk menggantikan algoritma DES yang dirasa sudah tidak aman lagi beberapa tahun lalu. Algoritma Blowfish adalah sebuah algoritma enkripsi simetris yang berarti bahwa algoritma ini menggunakan kunci yang sama baik untuk melakukan enkripsi dan dekripsi.

II. Studi Pustaka

Beberapa sumber referensi dari paper ini antara lain : paper berjudul Implementasi Algoritma RC6 Untuk Enkripsi SMS Pada Telepon Seluler yang dibuat oleh Rangga Wisnu Adi Permana, mahasiswa Teknik Informatika ITB, paper berjudul Penerapan Kode Huffman dan Kriptografi Pada Teknologi SMS yang dibuat oleh Auriga Herdinantio, mahasiswa Teknik Informatika ITB.

III. Metodologi Tugas Akhir

Karena aplikasi ini sederhana maka tidak dibutuhkan sutu kondisi yang rumit. Secara umum gambaran sistem adalah :

- Pengirim akan mengirim pesan melalui layanan SMS.
- Pesan ini akan dienkripsi terlebih dahulu sebelum dikirim.
- Pesan ini akan dikirim berupa pesan teks (Text Message).
- Pesan ini nantinya akan diterima oleh penerima pesan dalam keadaan terenkripsi.
- Karena pesan yang diterima dalam keadaan terenkripsi maka harus ada pendekripsi pesan supaya pesan yang diterima dapat dibaca.

Cara kerja sistem ini akan dibagi ke dalam beberapa tahapan proses supaya dapat dilihat dengan jelas. Tahapan proses dibagi menjadi empat tahapan sebelum tercipta sebuah sistem yang bisa digunakan untuk mengirimkan pesan via SMS dan pesan tersebut terenkripsi. Tahapan tersebut antara lain enkripsi pesan, pengiriman pesan, dekripsi pesan yang sudah diterima dan yang terakhir adalah proses penyimpanan pesan ke dalam inbox aplikasi. Untuk lebih jelasnya dapat dilihat pada gambar di bawah ini :

IV. Hasil Uji Coba

Tahap uji coba dibagi 3 :

1) User requirement : Persyaratan yang harus dimiliki oleh user adalah spesifikasi ponsel yang dimiliki harus mendukung Java MIDP 2.0 CLDC 1.1
2) Instalasi program : Proses instalasi program cukup mudah dilakukan. User hanya perlu mendownload/mengcopy file *.jar dari aplikasi ini. Ponsel akan otomatis melakukan instalasi. Kemudian kita bisa langsung menjalankannya.
3) Menjalankan program : Setelah masuk ke dalam aplikasi ini, pengirim dapat mengirimkan pesan dengan memilih menu 'Buat pesan baru' lalu mengetikkan nomer tujuan, pesan yang akan dikirim dan password, password maksimal 8 karakter. Setelah itu, pengirim dapat melakukan pengiriman pesan dengan menekan tombol 'Kirim'. Pesan yang dikirim akan ditampilkan langsung pada layar ponsel penerima dan siap untuk didekripsi. Sebelumnya pengirim harus memasukkan password supaya pesan dapat didekripsi. Kemudian penerima dapat memilih command 'Dekripsi' untuk mendekripsi pesan yang diterima.

Hasil percobaan :

- Pengujian dilakukan sebanyak 8 kali dengan jumlah karakter sms yang berbeda-beda.
- Contoh perhitungan nisbah/rasio kompresi : Total jumlah karakter sebelum mengalami proses enkripsi adalah 12. Total jumlah karakter setelah mengalami proses dekripsi adalah 10. Nisbah : (1-(10/12)) * 100% = (1-0.833) * 100 % = 16.7 %

No	Sebelum	Sesudah	Rasio (%)	Waktu (ms)
1	4	12	200	41
2	19	32	68.4	30
3	44	64	45.3	30
4	160	224	40	32
5	233	320	37.3	32
6	230	312	35.6	37
7	437	588	34.5	31
8	643	864	34.3	33

Rata-rata pembengkakan jumlah karakter pesan dari 8 buah data : 495.5/8 = 61.93 %

Rata-rata waktu dekripsi pesan dari 8 buah pesan : 266/8 = 33.25 ms

V. Kesimpulan

Berdasarkan hasil pengujian dan analisa yang telah di bahas pada bab sebelumnya maka dapat diberikan beberapa kesimpulan sebagai berikut :

1) Aplikasi ini berjalan dengan emulator Sony Ericsson untuk memudahkan pengujian.
2) Text yang diterima sama persis dengan text yang dikirim.
3) Aplikasi ini juga mampu berjalan pada ponsel sesungguhnya dan mampu melakukan proses enkripsi/dekripsi dengan baik.
4) Aplikasi ini mampu untuk melakukan proses enkripsi dan dekripsi pesan SMS menggunakan metode Blowfish. Namun, pesan yang telah dienkripsi memiliki jumlah karakter yang lebih banyak dibandingkan dengan jumlah karakter sebelum pesan tersebut dienkripsi. Hal ini mengakibatkan biaya pesan yang digunakan untuk melakukan pengiriman SMS lebih banyak jika dibandingkan dengan pengiriman SMS biasa. Namun jika dilihat dalam segi keamanan, maka aplikasi ini jelas lebih baik jika dibandingkan dengan pengiriman SMS biasa.

References

[1] Rengga, Krisna. 2009. Membuat Content Mobile Dengan J2ME. Jakarta. Penerbit Mitra Wacana Media.

[2] Herdinantio, Auriga. 2006. Penerapan Kode Huffman dan Kriptografi pada Teknologi SMS. Teknik Informatika ITB. Bandung.

[3] Wisnu Adi Permana, Rangga. 2007. Implementasi Algoritma RC6 Untuk Enkripsi SMS Pada Telepon Selular. Teknik Informatika ITB. Bandung.