STMIK GI MDP

Program Studi Teknik Informatika
Skripsi Sarjana Komputer
Semester Ganjil Tahun 2010/2011

STUDI PERBANDINGAN METODE HASH MD5, HUFFMAN DAN RC6 UNTUK PENGENKRIPSIAN DAN KOMPRESI DATA TEKS SMS

Ridwan Setiawan 2006250001
Yanto Sukardi 2006250021

Abstrak

Dunia saat ini terasa semakin maju dan berkembang. Semakin kita menikmati hidup, semakin juga kita dapat merasakan berkembangnya kemajuan berinteraksi antar sesama manusia. Dengan semakin majunya dunia, maka secara tidak langsung, teknologi komunikasipun terikut ambil peran/bagian dalam kepentingan dan kelangsungan hidup manusia. Berbagai cara, solusi, ide, ataupun karya-karya seseorang telah dimunculkan dan diciptakan. Salah satunya adalah dengan SMS(*Short Massage Service*) yang berupa suatu bentuk layanan dari fitur *handphone*/ ponsel serta operator jaringan yang berfungsi untuk bertukar informasi kepada sesama penggunanya. SMS bukanlah hal yang baru. Setiap orang di dunia yang terbiasa dengan penggunaan *handphone*/ponsel akan sangat mengenal dengan layanan SMS ini.Namun bukan berarti layanan ini mempunyai tingkat keamanan yang baik untuk bertukar informasi kepada sesama pengguna ponsel.
Tidak adanya pengamanan dari sistem SMS itu menjadi suatu hambatan tersendiri, baik dari ponsel maupun layanan operator jaringannya. Berbagai metode enkprisi telah diciptakan untuk digunakan sebagai pelindung isi dari pesan singkat tersebut dengan menggunakan kode rahasia. Setelah dienkripsikan, pesan singkat tersebut dapat dikompresikan sehingga ukuran bit-nya menjadi lebih kecil dan mampu menghemat memori ponsel ataupun memori kartu ponselnya. Maka dengan ini, penulis melakukan perbandingan antara metode HASH MD5, Huffman dan RC6 yang akan diterapkan pada sistem SMS lalu dicari manakah dari ketiga metode tersebut yang paling baik sesuai dengan indikatornya. Selain itu, penulis juga akan menyimpulkan hasil perbandingan tersebut dan menganalisa bahwa metode Huffman lebih baik dari pada yang lainya.

Kata kunci :

SMS(Short Massage Service), Enkripsi, Metode HASH MD5, HUFFMAN dan RC6

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Telepon seluler adalah media komunikasi yang paling popular saat ini dibandingkan surat, fax dan telepon umum. Karena selain praktis, telepon selular juga efisien dalam penggunaan waktu digunakan untuk kepentingan bisnis, usaha, pendidikan dan kepentingan pribadi. Telepon selular telah menjadi salah satu alat komunikasi tanpa batas waktu dan orang dengan mudah akan melakukan komunikasi di tempat-tempat yang diinginkan selain itu bahwa seseorang akan dapat melakukan pengiriman sms karena biaya yang sangat ekonomis yang ditawarkan pada masing-masing *domain* operator.

Short Message Service atau yang biasa disebut dengan SMS ini memiliki banyak kendala dalam keamanan sehingga kerahasiaan data akan mudah untuk dibaca atau disadap oleh seseorang yang tidak berhak mengetahui isi pesan tersebut. Hal tersebut yang sering dikenal dengan istilah *Hack* atau *Crack,* hal ini bisa terjadi karena ada unsur seperti dendam, persaingan bisnis dan lain-lain. SMS sebelum dikirimkan ke penerima akan ditampung didalam suatu *database* yang disebut dengan *Short Message Service Center* (SMSC). Celah keamanan yang besar dapat memudahkan seseorang yang tidak berkepentingan masuk,

membaca, mengambil dan merubah data yang penting dari seorang pengirim pesan.

Dengan kemajuan teknologi yang semakin berkembang telah diciptakan bermacam-macam metode enkripsi yang dapat membuat keamanan data semakin baik, metode dan algoritma yang disesuaikan dengan program yang ada. Enskripsi awalnya digunakan sebagai sandi untuk mengisyaratkan perang pada bangsa Yunani dalam sebuah gulungan. kode-kode enkrip tersebut dapat membentuk kata-kata atau kalimat- kalimat yang hanya diketahui oleh pembawa pesan dan penerima pesan. Macam-macam metode enskripsi yang digunakan pada perkembangan sekarang sebagai berikut: IDEA, MD4, MD5, RC 1-6, hufman, HASH, Enigma dan masih banyak lagi.

Penulis mencoba untuk memberikan, merumuskan dan membandingkan dari tiga metode tersebut yaitu HASH MD5, Huffman, RC6 yang ada karena dari tiga metode tersebut merupakan perkembangan dari metode-metode sebelumnya, untuk mengetahui dari segi keamanan yang manakah yang mampu memberikan keamanan lebih dan menjaga data agar tidak mudah untuk dicuri atau dibaca oleh orang yang tidak bertanggung jawab.

1.2 Perumusan Masalah

Permasalahan yang diangkat dalam Skripsi ini adalah manakah diantara algoritma HASH MD5, Huffman ,dan RC 6 yang menghasilkan pengenkripsian dan kompresi terbaik pada teks SMS.

1.3 Ruang Lingkup

Ruang lingkup dari laporan Penelitian Skripsi ini meliputi :

1. Bahasa pemograman yang digunakan adalah *Visual Basic* 6.
2. Variabel yang digunakan meliputi :
   a. Berupa data atau bilangan- bilangan setiap karakter dan kode-kode enkripsi.
   b. Ponsel GSM Nokia 5110 dan kabel data kits.
   c. Perangkat keras berupa laptop Axioo spesifikasi sebagai berikut:
      i. *Intel Pentium Core 2 duo*
      ii. *Memory* 3 Gb
      iii. *Hardisk* 250 Gb
      iv. VGA 256 MB
   d. CPU
      i. *Intel Pentium 4, 3.0 Ghz*
      ii. *Memory 512Mb*
      iii. *Hardisk 80 Gb*
   e. *Text message* yang bertipe *text mode* (dapat dibaca oleh mata manusia). Setiap karakter berupa angka dan huruf dapat dibaca oleh manusia sebagai pengguna dan dilakukan proses enkripsi dan kompresi.
   f. Penulis membatasi pada indikator berupa panjang karakter dan waktu proses sebagai pembanding antara metode hash MD 5, Huffman dan RC6.
   g. Dengan simulasi karakter SMS pada *Visual Basic* 6.0.

Metode-metode yang digunakan untuk perbandingan adalah sebagai berikut:

a. Algoritma HASH MD 5

   Sebuah metode dengan 4 penyangga yang dapat menampung data dengan bilangan *hexadecimal.*

b. Algoritma Huffman

   sebuah metode dengan menggunakan prefix kode yang memiliki bilangan bit'0' dan bit '1'

c. Algoritma RC6

   Sebuah metode yang diterapkan oleh Rivest dan merupakan salah satu kandidat AES (*Advanced Encryption Standard*). Dengan memecah blok 128 bit menjadi 4 blok 32 bit

1.4 Tujuan Dan Manfaat

A. Tujuan

Tujuan dari penelitian ini adalah untuk membandingkan 3(tiga) metode yang digunakan, yaitu : Hash MD5, Hufman dan RC6. Manakah Dari ketiga metode tersebut memiliki tingkat efisiensi yang lebih baik berdasakan waktu dan panjang karakter.

B. Manfaat

Manfaat yang dapat diambil dari penelitian ini ialah hasil dari perbandingan dari metode Hash MD 5, Huffman dan RC 6 untuk menjadi refrensi bagi pemogram dalam menentukan metode enkripsi dan kompresi.

1.5 Metodologi Penelitian

Dalam proses pengerjaan Penelitian ini terdiri dari langkah-langkah sebagai berikut:

1. Studi Literatur. Studi Literatur ini ditempuh dengan cara pengumpulan bahan – bahan berupa teori dan pemanfaatan informasi dari beberapa buku – buku ilmiah, pengumpulan data/sample langsung dari beberapa situs internet yang berhubungan dengan penulisan laporan Penelitian terutama buku – buku yang berhubungan langsung dengan penelitian ini.
2. Merancang tools yang digunakan sebagai alat bantu dalam melakukan perbandingan ketiga metode tersebut.
3. Penulis melakukan perbandingan metode-metode enkripsi dan kompresi menggunakan tools yang telah dibuat yang mengacu kepada indikator-indikator berikut:

   3.1 Waktu Dan Kecepatan Proses

   Waktu yang dibutuhkan dari ketiga metode yg digunakan untuk menyelesaikan proses pengenkripsian dan kompresi pada sms.

   3.2 Panjang Karakter Data

   Banyaknya data yang bisa dimasukan dengan menggunakan ketiga metode tersebut. Pengaruh banyaknya data yang dimasukan pada kinerja dari ketiga metode tersebut untuk sekali melakukan proses pengenkripsian dan kompresi pada sms.

   3.3 Jenis Karakter

Ketiga metode tersebut dapat membaca semua jenis karakter dan simbol yang digunakan pada saat proses pengenkripsian dilakukan.

4. Penulis melakukan analisa untuk menguji pendekatan kajian hasil dan menggunakan rumus- rumus perbandingan.
5. Kesimpulan dari hasil yang telah didapat dari penelitian ini.

Dengan menggunakan metode diatas diharapkan dapat menjadi acuan dalam mengerjakan penelitian dan memberikan hasil yang diharapkan dari penulis.

1.6 Sistematika Penulisan

Skripsi ini terdiri dari lima bab, berikut adalah sistematika penulisan skripsi :

BAB 1 PENDAHULUAN

Bab ini terbagi menjadi enam sub bab, yaitu Latar Belakang, Perumusan Masalah, Ruang Lingkup, Tujuan dan Manfaat, Metodologi Penelitian, serta Sistematika Penulisan.

BAB 2 LANDASAN TEORI

Bab ini berisi penjelasan dari sejarah singkat Kriptografi dan Enkripsi, Metode *Hash MD 5, Metode Huffman dan Metode RC 6* .

BAB 3 METODOLOGI PENELITIAN

Bab ini berisi penjelasan metodologi pemecahan masalah, *flowchart* program dan algoritma, spesifikasi file dan rancangan layar.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini membahas hasil dari penelitian yang dilakukan , prosedur uji coba penelitian, dan analisis hasil uji coba program dari penelitian tersebut.

BAB 5 PENUTUP

Bab ini berisi saran dan kesimpulan dari hasil perancangan dan pengujian yang dilakukan serta saran di akhir bab guna pengembangan penelitian ini lebih lanjut.

BAB 5

PENUTUP

5.1 Kesimpulan

Dari analisa yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Proses pengenkripsian di ukur Dari waktu , maka hasil yang lebih cepat adalah RC 6 di bandingkan dengan MD5 dan Huffman.
2. Proses pengenkripsian Diukur dari panjang karakter akhir dalam proses pengenkripsian adalah Huffman.
3. Proses Kompresi berdasarkan waktu adalah MD 5 lebih baik dibandingkan dengan Huffman dan RC6.
4. Berdasarkan Panjang karakter akhir adalah huffman dapat mengkompresi lebih baik dibandingkan dengan RC6 dan MD5.
5. Proses pengkompresian dan enkripsi RC6 dan MD 5 tetap menghasilkan 32 *Bytes*.

5.2 Saran

Beberapa saran yang dapat diberikan dari penelitian ini sebagai berikut:

1. Untuk memperoleh hasil lebih optimal dalam membaca pesan di dalam sistem komputer, sebaiknya digunakan spesifikasi yang ditulis oleh Penulis atau dengan spesifikasi yang lebih tinggi.
2. Untuk peneliti selanjutnya, diharapkan dapat menggunakan bahasa pemograman lain dan dapat diterapkan berbagai kunci untuk keamanan
3. Untuk peneliti selanjutnya, diharapkan dapat menggunakan algoritma-algoritma baru dalam penerapan.
4. Disarankan untuk mengambil algoritma pengenkripsian terbaik dan dilakukan proses dekripsinya untuk tahap selanjutnya.
5. Untuk peneliti selanjutnya, diharapkan menggunakan dari ketiga algoritma tersebut untuk keamanan pada SMS.