APLIKASI CHAOTIC CRYPTOGRAPHY PADA SMS

Sri Prima Retnowati[1], Dewi Utami Mt. ; Danang Mursita Msi[2], [3]

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

Abstrak

Kata Kunci :

Abstract

Keywords :

BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

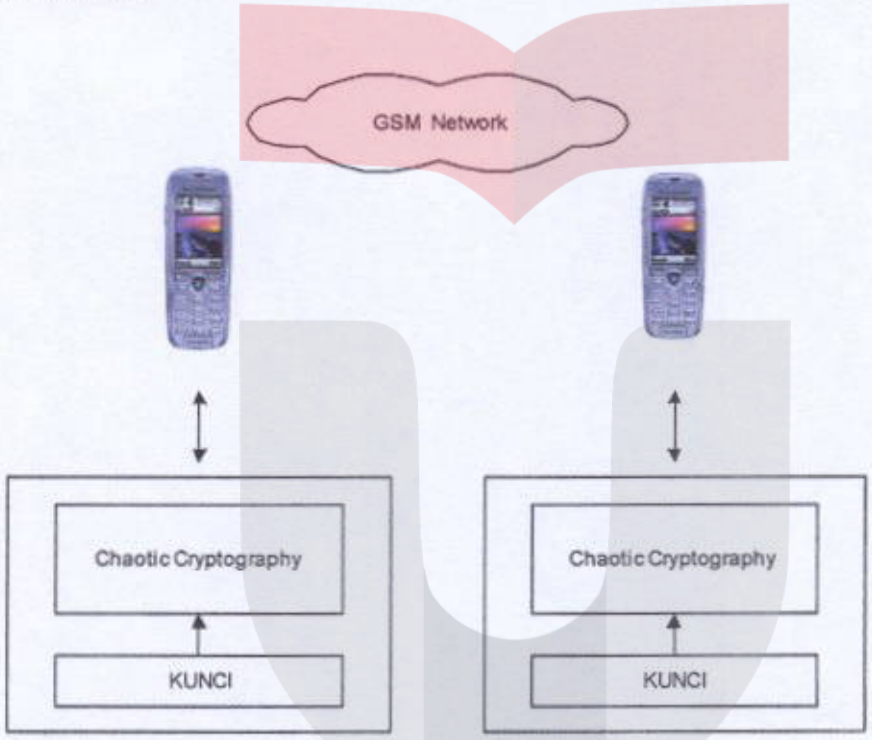
Kebutuhan akan informasi yang cepat dan akurat kini dirasakan sangat penting bagi berbagai kalangan. Tiap orang bebas mengakses informasi yang diinginkan. Alat-alat pendukung untuk memperoleh informasi kini telah banyak tersedia dan makin banyak ragamnya sesuai dengan tingkat kehandalannya. Namun, tanpa disadari segala kemudahan akses ini mampu memicu seseorang untuk melakukan akses gelap terhadap data-data yang bersifat rahasia. Kita tidak akan pernah tahu siapa saja yang berniat untuk membobol sistem pertahanan data base sebuah bank, atau siapa yang menyadap informasi-informasi rahasia dari Kepolisian.

Oleh sebab itu kita perlu memikirkan bagaimana caranya agar informasi yang kita kirimkan dapat aman dari gangguan para penyelundup. Disinilah peran kriptografi. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Bagian-bagian dari kriptografi adalah enkripsi dan dekripsi. **Enkripsi** adalah sebuah proses encoding suatu pesan sehingga arti pesan menjadi tidak nyata; sedangkan **dekripsi** adalah proses kebalikannya. Yaitu transformasi pesan terenkripsi menjadi bentuk normal. Secara bergantian, encode dan decode atau enchiper and dechiper digunakan. Sebuah system untuk enkripsi dan dekripsi disebut ***cryptosystem***.[1]

Kini berbagai metode enkripsi telah digunakan secara luas contohnya seperti DES, RSA dan sebagainya. Di dalam Tugas Akhir ini akan dicoba menggunakan metode enkripsi chaotic sebagai harapan baru untuk metode enkripsi yang lebih baik. Di sini juga akan dicoba untuk mengaplikasikan metode enkripsi chaotic ke dalam text SMS (Short Message Service).SMS yang kita kirimkan dapat dengan mudah dibaca dengan menggunakan alat tapping SMS. Titik-titik yang rawan bagi pengiriman SMS yaitu pada bagian SMSC- MSC. SMS dan MSC dapat digunakan untuk menangkap isi SMS seseorang. Pada SMSC terdapat elemen buffer sebagai penyimpan SMS yang datang.

1.2. Perumusan Masalah

Ide dari Tugas Akhir ini adalah bagaimana mengaplikasikan *Chaotic Cryptography* ke dalam *Short Message Service* (SMS). Sehingga, pesan-pesan rahasia yang kita kirimkan akan tetap aman. Untuk mengenkrip text SMS digunakan enkripsi chaotic. Berikut ini adalah blok diagram enkripsi SMS yang akan di implementasikan pada tugas akhir ini.



Gambar 1.1 Blok perancangan Chaotic Cryptography pada SMS

Dalam sistem tersebut akan digunakan algoritma kriptografi simetris kategori *stream cipher*. Dimana pada algoritma aliran (stream cipher), proses penyandiannya berorientasi pada satu bit atau satu byte data. Hal ini untuk menghindari waktu pemrosesan yang terlalu lama. Teknologi untuk sistem wireless yang digunakan adalah J2ME (*Java 2 Micro Edition*).

1.3. Batasan Masalah

Dalam penulisan Tugas Akhir ini masalah yang akan dibahas akan dibatasi sebagai berikut:

1. Pesan yang dikirim berupa text SMS dari GSM.
2. Metode yang digunakan adalah Chaotic Cryptography dengan fungsi Modulo sebagai pembangkit sinyal Chaos.
3. Handphone yang bisa digunakan adalah Handphone yang berbasis Java dengan teknologi MIDP 2.0. Dalam hal ini, penulis menggunakan Sony Ericsson K500i.

1.4. Tujuan Pembahasan

Tujuan dari penulisan Tugas Akhir ini antara lain:

1. Mengimplementasikan algoritma enkripsi chaotic dengan menggunakan *Java 2 Micro Edition programming*.
2. Mengetahui apakah enkripsi chaotic cukup aplikatif berdasarkan data hasil ujicoba.
3. Mengetahui apakah data enkripsi dapat ditransmisikan melalui Short Message Service GSM.

1.5. Metode Penelitian

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

- Metode Deskriptif
  Studi Literatur, ini dimaksudkan untuk mencari dan mempelajari konsep dari teori pendukung terhadap implementasi sistem.
- Metode Eksperimental
  Dengan mencoba merealisasikan sistem ke dalam device yang akan digunakan.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Menjelaskan mengenai latar belakang masalah, rumusan masalah yang akan dianalisa, pembatasan masalah, tujuan pembuatan sistem, dan menentukan metode pemecahan masalah dari sistem serta sistematika peulisan.

BAB II LANDASAN TEORI

Memuat teori tentang Chaos dan teori lain yang mendukung terlaksananya pengembangan sistem ini.

BAB III PERANCANGAN DAN PENGIMPLEMENTASIAN SISTEM ENKRIPSI SMS

Membahas rancangan dari sistem yang akan dibuat, penerapan algoritma enkripsi, pemrograman untuk mengaplikasikan enkripsi sms.

BAB IV PENGUJIAN DAN ANALISA ENKRIPSI SMS

Berisi tentang pengujian sistem dan analisa hasil implementasi enkripsi chaos yang telah diaplikasikan ke dalam sms.

BAB V PENUTUP

Berisi kesimpulan yang dapat diambil dari keseluruhan sistem yang dibuat serta saran-saran untuk perbaikan dan kemungkinan pengembangan.

BAB V
PENUTUP

5.1. Kesimpulan

1. Dengan menggunakan fungsi modulo sebagai fungsi non linier pembangkit sinyal chaos, ternyata *chaotic cryptosystem* menjadi lebih mudah diimplementasikan karena tidak lagi membutuhkan fungsi invers.
2. Karena saat sampai saat ini J2ME dengan MIDP 2.0 (Versi terbaru) masih belum mendukung implementasi dengan floating point, maka setelah chaotic generator ini diimplementasikan ke dalam *mobile phone* tingkat presisinya menjadi berkurang.
3. Implementasi dilakukan dengan memasukkan kombinasi kunci dengan harga – harga integer saja, sehingga resikonya adalah enkripsi ini akan lebih mudah dipatahkan.

5.2. Saran

Saran – saran untuk pengembangan lebih lanjut dari system pengenkripsian SMS ini adalah :

1. Untuk pengembangan aplikasi ke sistem wireless dapat dilakukan jika perbaikan pada J2ME versi berikutnya mampu *men-support floating point*.
2. Masih banyak metoda Chaos yang lebih kompleks untuk meningkatkan tingkat keamanan.
3. Untuk selanjutnya dapat dikembangkan implementasi untuk mengenkripsi image dan voice

DAFTAR PUSTAKA

[1] A.M. Dabrowski, W.R. Dabrowski, M.J.Ogorzalek, *Dynamic Phenomena in Chain Interconnection of Chua's Circuit*, IEEE Transaction on Circuits and System, Vol.40, No.11, pp.868-871, November 1993.

[2] Silva, C.P., Young, A.M. "Introduction to chaos-based communications and signal processing". *IEEE Aerospace Conference Proceedings, 2000*, vol.1 pp. 279-299.

[3] Pecora, L.M., Carroll, T.L. "Synchronization in Chaotic Systems" *Physical Review Letters*, vol. 64, pp. 821-824, 19 Feb. 1990.

[4] Frey, D.R. "Chaotic Digital Encoding: An Approach To Secure Communication" *IEEE Transactions on Circuits and Systems*, vol. 40, no.10, pp.660-666, October 1993.

[5] Utami Dewi; " Pengembangan Perangkat Keras Sistem Kriptografi Dengan Menggunakan Sinyal Chaos"; Tesis Magister Program Pasca Sarjana; ITB; 2001

[6] Gotz Marco; Kelber K.; Schwarz, W; "Generation of chaotic signals with n-dimensional uniform probability distribution by digital filter structures"

[7] Denny Gulick, "Encounters With Chaos", Mac Graw Hill, 1992

[8] Kelber Kristina, Wolfgang Schwarz, *Digital Realization of Discrete Time Chaos Generators.*

[9] Marco Gotz, *Non Linier Digital Waveform Coding of Chaotic Signals*, Technische Universitat Dresden, 1998.

[10] Team GSM, "Modul Open Mind Technology and Application", Mobile Communication Laboratory STT Telkom, 2003

[11] Thomas Falk, Marco Gotz, *A Chaos Based Programmable Analogue Digital Circuit for Broadband Signal Generator*, Technische Universitat Dresden, 1998

[12] Wicaksono Ady, 2003, *Pemrograman Aplikasi Wireless dengan Java*, Jakarta, Elex Media Komputindo

[13] Schneier Bruce, 1996, *Applied Cryptography*, 2nd Edition, Canada, John Wiley&Sons,Inc.