Jurusan Teknik Informatika

Skripsi Sarjana Komputer

Semester Genap tahun 2000/2001

CRYPTOGRAPHY DENGAN *CHAOS THEORY*

Frans Indroyono 0331970535

Kelas : 08PAT

Abstrak

Chaos theory adalah cabang ilmu matematika yang mempelajari tentang sistem yang sangat bergantung pada keadaan awal. Cuaca, ekologi, perekonomian, kemasyarakatan, reaksi kimia dalam tubuh, otak adalah beberapa contoh *chaotic system*. *Chaos theory* ditemukan pada tahun 1960 oleh Edward Lorentz.

Random number generator yang baik merupakan salah satu kebutuhan dalam merancang *cryptosystem*. Gejolak alam adalah sumber *random number* terbaik. *Logistic function* sebagai contoh sederhana sebuah *chaotic system* dipakai sebagai *random number generator* dalam dua *cryptosystem* yang dibahas dalam skripsi ini yaitu *SimplyChaos-X2* dan *MagicTable214*.

Dengan melihat perbandingan antara beberapa *cipher text* dan *plain text* dan melakukan pembuktian matematis, dapat disimpulkan bahwa kedua *cryptosystem* bersifat *unconditionally secure*.

Kata kunci

cryptography, chaos theory, passphrase analyzer, logistic function, ground effect, unconditionally secure, one-time pad cipher, polyalphabetic cipher.

PRAKATA

Ketertarikan saya pada *cryptography* berawal 2 tahun lalu dalam eksperimen kecil di kamar. Sejak itu saya mulai mencari dan mempelajari *cryptography*. Setengah tahun pertama saya tidak mendapatkan apa-apa karena hampir semua teman saya tidak tahu tentang *cryptography* kecuali sahabat saya, Jehoshua. Setelah saya membicarakan *cryptography* dengan Jehoshua, pengertian dan pemahaman kami tentang *cryptography* mulai berkembang. Bahkan, meskipun dibatalkan karena jadwal kuliah yang padat, kami sempat menawarkan diri untuk melakukan *research* bersama kepada Dr. Sarwono Soetikno, seorang dosen di ITB.

Dalam 1,5 tahun terakhir, kami tidak menggarap skripsi bersama. Saya mulai menggeluti *number theory* dan *chaos theory* untuk mendalami *cryptography* dan Jehoshua mendalami *digital certificate*, *PKI* dan banyak hal tentang *cryptography*. Semua itu kami lakukan sendiri, otodidak melalui buku-buku dan kami tetap saling berbagi paper, dokumentasi, *treatise* mengenai *cryptography* dan perkembangan masing-masing.

Selama saya menggarap skripsi, saya banyak melakukan pemrograman untuk analisa yang lebih dalam, pengujian dan revisi *cryptosystem*. Penemuan pemecahan masalah selalu membuat saya gembira, terlebih lagi setelah melihat bahwa kedua *cryptosystem* selesai ditulis, bekerja dengan sempurna dan terutama karena keduanya *unconditionally secure*.

Penemuan teknik *Ground Effect Passphrase Analyzer* (GEPA) adalah salah satu hasil dari banyak analisa dan pengujian yang saya lakukan selama ini. Tekniknya diilhami dari peristiwa *ground effect* dalam dunia aerodinamika yang secara tidak sengaja saya lihat di TV. GEPA adalah *passphrase analyzer* yang mampu menghasilkan *entropy*

ideal untuk setiap *passphrase* yang diberikan. Selain itu saya menemukan bahwa *chaos theory* adalah ilmu yang sangat menarik di samping psikologi. Karena kita bisa lebih memahami mengapa dan bagaimana suatu peristiwa terjadi, khususnya peristiwa yang hingga saat ini belum bisa dipahami seperti peramalan cuaca dan terbentuknya kehidupan.

Saya berharap hasil kerja saya bisa memicu pengembangan *cryptography* dan minat pada *chaos theory* di Indonesia. Saya juga mengucapkan terima kasih kepada:

1. Kedua orang tua yang membesarkan saya, memberi saya kesempatan dan membelikan buku-buku.
2. Rektor Universitas Bina Nusantara Ir. Th. Widia S., MM.
3. Ketua Jurusan Teknik Informatika Sablin Yusuf, Ir., M.Sc., M. CompSc.
4. Sekretaris Jurusan Teknik Informatika Januar Wahjudi, S.Kom., M.Sc.
5. Dosen pembimbing skripsi Ir. Samuel Lukas M.Tech atas bantuannya dalam membuat pembuktian dan usahanya memahami *cryptosystem* yang dibahas.
6. Akin, sahabat yang selalu ada di sisi saya dan orang yang mengawali semua yang saya lakukan. Terima kasih atas ide, saran dan pertanyaan yang tidak terpikirkan sebelumnya.
7. Jehoshua, sahabat yang selalu berbagi ide, informasi, memberi dukungan moral, analisa.
8. Carinnia, adik angkat yang selalu mendukung saya.
9. Lara Davis, kakak yang mewarnai hidup saya.
10. Jared Cole, teman jauh yang membuat saya mengerti perbedaan antara *semi-random* dan *true random*.
11. Pak Makmuri, dosen matematika diskrit dan kalkulus lanjut. Orang yang meminjamkan buku "*Elementary Number Theory*", memberi dukungan.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GRAFIK

DAFTAR GAMBAR

DAFTAR LAMPIRAN