PENGANTAR ILMU KRIPTOGRAFI TEORI, ANALISIS, DAN IMPLEMENTASI

Ade Anshori[1], Niken Dwi Cahyani[2], Endro Ariyanto[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Twofish merupakan algoritma pengembangan dari Blowfish, namun Blowfish memiliki beberapa keunggulan dibandingkan dengan Twofish. Salah satu keunggulan adalah pada performansi waktu proses enkripsi dan dekripsi, dimana Blowfish lebih cepat waktu proses enkripsi dan dekripsi daripada Twofish. Untuk besar file input dan output kedua algoritma tidak memiliki keunggulan masing-masing, dimana besar file ciphertext baik Blowfish dan Twofish dapat menghasilkan besar yang sama maupun berbeda sedikit lebih besar atau lebih kecil. Nilai avalanche effect Twofish menghasilkan nilai yang lebih baik daripada Blowfish, hal ini dikarenakan pada Twofish terdapat tingkat pengacakan dan penambahan algoritma yang lebih rumit.

Kata Kunci : Blowfish, Twofish, Ciphertext, Avalanche Effect

Abstract

Twofish is the development of the Blowfish algorithm, but Blowfish has several advantages compared with Twofish. One advantage is the performance period for the encryption and decryption, where faster time Blowfish encryption and decryption process than Twofish. To a large input and output files both algorithms do not have the advantages of each, where both large ciphertext files Blowfish and Twofish can produce the same magnitude and differ slightly larger or smaller. Value Twofish avalanche effect produces a better value than Blowfish, this is due to the Twofish randomization rate and the addition of a more complex algorithm

Keywords : Blowfish, Twofish, Ciphertext, Avalanche Effect

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada umumnya, perancangan suatu algoritma enkripsi harus dapat memenuhi kebutuhan pengguna yaitu memiliki karakteristik cepat, kuat, sederhana dan tidak terhalang lisensi. Blowfish merupakan salah satu algoritma yang diciptakan oleh Bruce Schneier pada tahun 1993, perancangannya dimaksud untuk menggantikan *Data Encryption Standard* (DES) dan dapat memenuhi karakteristik di atas. Blowfish kemudian dapat menarik perhatian publik dan dianggap sebagai algoritma terbaik karena telah digunakan dalam dunia open source sebagai *Open Cryptography Interface* (OCI) pada kernel Linux versi 2.5 ke atas.

Seiring berkembangnya algoritma enkripsi kesuksesan Blowfish mulai memudar, karena pada saat pengimplementasiannya Blowfish tidak cocok untuk aplikasi yang sering memerlukan perubahan kunci. Sehingga Bruce Schneier melakukan pengembangan algoritma Blowfish menjadi algoritma Twofish dan berhasil masuk menjadi lima kandidat algoritma standar enkripsi *Advanced Encryption Standard* (AES). Tujuan perancangan Twofish sendiri agar dapat digunakan secara efisien baik pada software maupun hardware, rancangan yang sederhana dan mudah diimplementasikan. Twofish juga diharapkan dapat memenuhi kebutuhan pengguna dalam aplikasi enkripsi, serta memiliki kelebihan performansi dari algoritma Blowfish.

Algoritma Blowfish dan Twofish merupakan algoritma enkripsi yang kuat dan masih banyak digunakan dalam aplikasi enkripsi, namun dalam pengimplementasiannya harus disesuaikan dengan kebutuhan pengguna. Alasan pemilihan kedua algoritma di atas karena algoritma Blowfish dan Twofish memiliki hubungan yang sangat erat diantaranya Twofish merupakan perkembangan dari Blowfish, keduanya sama-sama tergolong jenis algoritma cipher blok, dirancang oleh orang yang sama (Bruce Schneier) dan dalam proses enkripsinya kedua algoritma tersebut menggunakan jaringan feistel.

Secara umum, Twofish dirancang agar lebih baik dan lebih unggul daripada Blowfish, namun sebaik dan seunggul apakah Twofish dibandingkan dengan Blowfish dari sisi perbedaan performansi yang akan dianalisis. Dengan adanya permasalahan di atas, maka pada Tugas Akhir ini akan dilakukan penelitian yang bertujuan untuk menentukan kelebihan dan kekurangan algoritma Blowfish dan Twofish berdasarkan kebutuhan pengguna. Penelitian akan dilakukan berdasarkan perbandingan performansi yang dihasilkan kedua algoritma. Implementasi Tugas Akhir ini akan menggunakan Visual Basic 6.0 sebagai media perbandingan performansi enkripsi dan dekripsi data.

1.2 Perumusan Masalah

Blowfish dan Twofish merupakan algoritma kripografi kunci simetri dan juga merupakan cipher blok. Permasalahan yang dijadikan objek penelitian dan pengembangan tugas akhir ini adalah:

1. Bagaimana mekanisme kerja enkripsi dan dekripsi data dengan menggunakan algoritma Blowfish dan Twofish.
2. Bagaimana perbandingan performansi algoritma Blowfish dan Twofish berdasarkan parameter waktu proses enkripsi dan dekripsi, perbandingan besar file input / output enkripsi dan dekripsi, nilai *avalanche effect* enkripsi dan dekripsi.

1.3 Tujuan Penulisan

Tujuan penulisan dari Tugas Akhir ini sebagai berikut :

1. Menghasilkan suatu perangkat lunak yang dapat menghasilkan perbandingan performansi antara algoritma Blowfish dan Twofish, sehingga dapat dilihat performansi masing-masing algoritma berdasarkan parameter perbandingan yang dianalisa.
2. Menganalisis perbandingan performansi (waktu proses enkripsi/dekripsi, perbedaan besar file input/output, nilai *avalanche effect*) algoritma Blowfish dan Twofish.

1.4 Batasan Masalah

Batasan masalah dalam membandingkan algoritma Blowfish dan Twofish pada tugas akhir ini adalah :

1. File inputan yang digunakan adalah file teks atau tulisan.
2. Parameter ukuran yang dianalisa adalah :
    a. Waktu proses enkripsi dan dekripsi.
    b. Perbedaan besar file input dan output.
    c. Nilai *Avalanche Effect*.

1.5 Metodologi Penulisan

Metodologi yang digunakan untuk menyelesaikan masalah dalam Tugas Akhir ini adalah

1. Studi Literatur
   Studi literatur dari beberapa buku, jurnal, artikel yang membahas tentang tipe file teks, kriptografi, algoritma cipher blok, kunci simetri, blowfish, twofish dan karakteristik serta pembuatan aplikasi.
2. Analisis dan Desain
   Tahap ini meliputi analisis kebutuhan serta penyelesaian masalah untuk merancang perangkat lunak enkripsi dan dekripsi file teks dengan menggunakan

algoritma Blowfish dan Twofish. Desain perangkat lunak yang akan dibangun berdasarkan proses.

3. Perancangan dan Implementasi Sistem
   Tahap ini meliputi pembangunan perangkat lunak yang telah dirancang pada tahap sebelumnya. Pembangunan perangkat lunak menggunakan Visual Basic 6.0.
4. Analisis dan Pengujian
   Pada tahap ini adalah melakukan analisis terhadap hasil pengujian perangkat lunak dalam enkripsi pada file. Untuk mengukur waktu, besar file input/output, nilai *avalanche effect* dengan menggunakan ukuran file teks dan panjang kunci yang berbeda-beda. Sehingga didapatkan rata-rata perbedaan performansi kedua algoritma. Analisa dan perhitungan keluaran dari sistem yang telah dibangun.
5. Penyusunan Laporan
   Hasil penelitian akan disusun menjadi suatu laporan yang meliputi aspek-aspek dalam penelitian yaitu teori, perancangan dan implementasinya, serta membuat kesimpulan dan saran dari hasil penelitian

1.6 Sistem Penulisan

Struktur Pembahasan Tugas Akhir ini disusun berdasarkan Sistematika Penulisan sebagai berikut :

BAB I. Pendahuluan

Dalam pendahuluan akan dijelaskan secara singkat latar belakang, perumusan masalah, tujuan penulisan, batasan masalah, metoda penelitian dan sistematika penulisan.

BAB II. Landasan Teori

Pada bab ini akan dijelaskan tentang algoritma kunci simetri, teori dan implementasi sistem, penjelasan algoritma Blowfish dan Twofish, konsep dasar kedua algoritma serta metode enkripsi cipher blok, metode perhitungan waktu, besar file, *avalanche effect*.

BAB III. Analisis Desain dan Perancangan Sistem

Bab ini berisi analisis terhadap seluruh masalah seperti kebutuhan perangkat lunak, dan membahas mengenai perancangan perangkat lunak sistem

BAB IV. Implementasi dan Analisis Hasil Pengujian

Bab ini berisi implementasi dari sistem yang dibuat, dan melakukan analisa hasil pengujian aplikasi yang dibuat berdasarkan waktu, besar file input/output, *avalanche effect*.

BAB V. Kesimpulan dan Saran

Pada bab akhir terdapat kesimpulan dari seluruh rangkaian penelitian yang dilakukan dan saran untuk pengembangan selanjutnya.

BAB V

KESIMPULAN DAN SARAN

Pada bab ini, akan disimpulkan hasil dari seluruh uraian yang telah dijelaskan mulai dari tahap analisis sampai tahap implementasi dan memberikan saran-saran yang membangun.

5.1 Kesimpulan

1. Waktu proses enkripsi dan dekripsi algoritma Blowfish waktu proses lebih cepat daripada Twofish. Hal ini dikarenakan pada algoritma Twofish memiliki tingkat pengacakan dan penambahan algoritma yang lebih rumit dibandingkan dengan Blowfish.
2. Ukuran file output (*ciphertext*) hasil enkripsi dan dekripsi baik Blowfish dan Twofish menghasilkan besar *ciphertext* yang sama, lebih besar atau lebih kecil. Hal ini dikarenakan penambahan bit dipengaruhi oleh proses *padding* yaitu penambahan bit pada blok yang sisa atau bukan kelipatan blok bit. Pada Blowfish blok bit adalah 64 bit dan Twofish blok bit adalah 128 bit.
3. Ukuran kunci yang digunakan tidak mempengaruhi waktu proses serta besar file input dan output proses enkripsi dan dekripsi baik Blowfish maupun Twofish. Hal ini dikarenakan kunci yang diinputkan akan dibangkitkan menjadi subkunci-subkunci yang memiliki panjang yang telah ditentukan.
4. Nilai *avalanche effect* pada Blowfish dan Twofish sama-sama memiliki nilai yang baik yaitu antara 40%-60 % atau mendekati 50%. Tetapi nilai *avalanche effect* Twofish masih lebih baik

5.2 Saran

1. Perbandingan dapat dilakukan dengan menggunakan mode operasi cipher blok lain seperti : ECB, OFB dan CFB
2. Algoritma ini dapat diimplementasikan dalam berbagai hal, misalkan: enkripsi/dekripsi secara realtime
3. Menganalisis Blowfish dan Twofish dari sisi keamanan (kriptanalisis).

DAFTAR PUSTAKA

[1] Munir, Rinaldi. (2004). *Bahan kuliah IF5054 Kriptografi*, Departemen Teknik Informatika, Institut Teknologi Bandung.

[2] Wikipedia (2006). http://en.wikipedia.org/wiki/Cryptography Tanggal Akses : 20 Oktober 2009

[3] Wikipedia (2006). http://en.wikipedia.org/wiki/Symmetric-key_algorithm. Tanggal Akses : 20 Oktober 2009.

[4] Wikipedia (2006). http://en.wikipedia.org/wiki/Block_cipher. Tanggal Akses : 22 Oktober 2009.

[5] Wikipedia (2006). http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation. Tanggal Akses : 22 Oktober 2009.

[6] Wikipedia (2006). http://en.wikipedia.org/wiki/Twofish. Tanggal Akses : 23 Oktober 2009.

[7] Wikipedia (2006). http://en.wikipedia.org/wiki/Blowfish_(cipher). Tanggal Akses : 23 Oktober 2009.

[8] Bruce Schneier (1994), http://www.schneier.com/twofish.html. Tanggal Akses : 24 Oktober 2009.

[9] Wikipedia (2006). http://en.wikipedia.org/wiki/Feistel_cipher. Tanggal Akses : 25 Oktober 2009.

[10] Schneier, Bruce, *Applied Cryptography 2nd*, John Wiley & Son, 1996.

[11] Ariyus, Dony (2008), *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*, STMIK AMIKOM. Yogyakarta.

[12] Al Tamimi, Abdel-Karim, http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html. Tanggal Akses : 01 November 2009.

[13] Manurung, Fernando (2008), *Tugas Akhir "Enkripsi Gambar Dengan Menggunakan Algoritma Enhance 1-D Chaotic Key Based (ECKBA)"*. Institut Teknologi Telkom. Bandung.

[14] Trisnawati (2007), Tugas Akhir Mata Kuliah Keamanan Jaringan Komputer "*Sistem Keamanan Menggunakan Algoritma Blowfish Advance CS Pada File dan Folder Data*", Universitas Sriwijaya

[15] Mukmin, Indra. "Algoritma Twofish : kinerja dan implementasinya sebagai salah satu kandidat algoritma AES (Advanced Encryption Standard)", Institut Teknologi Bandung. Bandung

[16] Ferguson, Niels (1998)"Twofish: A 128-Bit Block Cipher", University of California