ANALISIS HASIL IMPLEMENTASI ALGORITMA KRIPTOGRAFI MARS UNTUK FILE MP3

Dewi Rosaria Eva Mayestika[1], M. Zuliansyah[2], Vera Suryani[3]

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

Abstrak

Saat ini industri musik Indonesia berkembang pesat. Pada industri musik umumnya informasi yang digunakan adalah file audio. Hal ini menyebabkan aktivitas pengiriman dan penyimpanan file audio pun sering dilakukan sehingga kerahasiaan dari isi file audio tersebut perlu dijaga. Salah satu cara untuk menjaga kerahasiaan file audio adalah dengan menyandikan data tersebut ke dalam bentuk yang tidak dapat dimengerti informasinya. Penyandian data tersebut terdiri dari dua proses, yaitu enkripsi dan dekripsi.

Dalam tugas akhir ini diimplementasikan algoritma kriptografi Mars untuk penyandian data. Analisis hasil implementasi dilakukan dengan cara penilaian obyektif dan subyektif. Penilaian secara obyektif dilakukan untuk menganalisis perubahan ukuran file input, waktu penyandian data, dan properti file audio dengan menghitung besar perubahan ukuran file, menghitung waktu proses enkripsi dan dekripsi data, serta menggambarkan grafik sinyal file audio. Sedangkan penilaian secara subyektif dilakukan untuk mengetahui pita suara file audio hasil dekripsi dengan menggunakan pendengaran manusia.

Dari pengujian menunjukkan bahwa ukuran file akan bertambah sebesar 20 byte setelah proses enkripsi, waktu proses dekripsi file lebih lama dari proses enkripsinya, dan properti file audio hasil proses sama dengan aslinya.

Kata Kunci : enkripsi, dekripsi, file audio, algoritma kriptografi Mars

Abstract

Nowdays music industry in Indonesia has been developing. In music industry, commonly information which is usually used, is audio file. This causes sending and storaging activity of audio file almost be used, hence security of audio file mus be protected. To protect the security of audio file, we must do an encryption data becomes unidentifying form of information. This encryption consists of two process, which is encryption and decryption

In this final project has been implemented an Mars cryptography algorithm to encrypt data. Analysis of implementation result has been done in two ways, which is objective and subjective way. In objective way, we analyze the changing of file input size, time of encryption, and property of audio file by calculating the changing of file input size, time of encryption and decryption process and drawing signal graphic of file audio. While, in subjective way we analyze vocal chord of file audio from decryption result in human hearing.

From testing shows size of file will increase 20 bytes after encryption process, time of file decryption longer than encryption process and result of property of audio file same with the original.

Keywords : encryption, decryption, audio file, Mars Crypthography Algorithm

1. Pendahuluan

1.1 Latar belakang

Saat ini industri musik tanah air sedang berkembang pesat. Umumnya informasi industri musik berupa file audio. Aktivitas pengiriman dan penyimpanan file audio pun sering dilakukan. File audio yang umumnya dipakai adalah mp3 yang mana dari segi ukuran file relatif kecil, meskipun tergantung file itu sendiri. MP3 (MPEG Audio Layer-3) adalah format file MPEG (*Motion Pictures Expert Group*). MPEG adalah format standar dalam penyimpanan dan pendistribusian data multimedia terkompresi. Kerahasiaan dari isi file audio perlu dijaga seiring dengan semakin tingginya persaingan di industri musik. Salah satu teknik yang dapat digunakan untuk menjaga kerahasiaan data adalah dengan penyandian data. Penyandian data terdiri dari dua proses, yaitu enkripsi dan dekripsi.

Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

File mp3 memiliki struktur yang berbeda dengan file multimedia lainnya. Perbedaannya terletak pada header dari tiap frame file mp3 yang harus selalu tersimpan pada awal data, sehingga file mp3 harus dipartisi sesuai ukuran dari tiap framenya. Oleh karena itu mode operasi partisi blok yang sesuai untuk file mp3 adalah mode operasi CBC (*Cipher Block Chaining*). Dengan penggunaan mode tersebut penambahan bit pading pada frame file mp3 tidak perlu dilakukan, karena apabila terdapat bit sisa dapat dilakukan operasi XOR dengan *initialization vector* (IV).

National Institute of *Standard and Technology* (NIST) adalah lembaga yang bertugas untuk menilai algoritma-algoritma yang sudah masuk sebagai kandidat untuk AES dengan kriteria kunci yang digunakan harus panjang, ukuran blok yang digunakan harus lebih besar, lebih cepat, dan fleksibel. Tabel berikut merupakan hasil penilaian NIST terhadap 5 finalis AES, dimana dari tabel berikut dapat dilihat bahwa algorutma MARS memiliki rata-rata nilai yang stabil dibanding dengan keempat algoritma lainnya. [8]

Tabel 1-1: Metrik Penilaian 5 Finalis AES Berdasarkan Parameter NIST

Metric/Algoritma	MARS	RC6™	Rijndael	Serpent	Twofish
Algoritma Design & Presentation (10 point)	8	10	8	8	8
Security (30 point)	28	29	25	28	27
Ease of Implementation (10 point)	8	9	7	8	7
Usage Flexibility (10 point)	8	8	7	8	8
Performance/Efficiency (10 point)	8	9	8	7	9
Performance on Smart Card (10 point)	8	7	9	9	8
Strength against Crypanalisis (10 point)	8	9	7	8	9
FutureResilience (10 point)	8	8	7	9	8
Total (Max 100)	84	89	78	85	84

1.2 Perumusan masalah

Masalah yang akan diteliti berdasarkan latar belakang adalah sebagai berikut :

1. Bagaimana menerapkan proses enkripsi data dengan algoritma MARS.
2. Bagaimana menerapkan proses dekripsi data dengan algoritma MARS.
3. Apakah terdapat perbedaan properti suara yang meliputi frekuensi, amplitudo dan pita suara setelah dilakukan proses enkripsi dan dekripsi data dengan algoritma Mars.
4. Apakah terdapat perbedaan ukuran file setelah di lakukan proses enkripsi dan dekripsi data.

Dalam Tugas akhir ini, rumusan masalah tersebut dibatasi dengan ruang lingkup sebagai berikut :

1. Panjang kunci yang digunakan adalah 128 bit.
2. Fungsi hash yang digunakan adalah SHA-1.

1.3 Tujuan

Tujuan yang ingin dicapai dalam Tugas akhir ini adalah :

1. Dapat mengimplementasikan proses enkripsi data dengan algoritma kriptografi Mars ke dalam perangkat lunak.
2. Dapat mengimplementasikan proses dekripsi data dengan algoritma kriptografi MARS ke dalam perangkat lunak.

3. Mengetahui properti suara dari file mp3 yang meliputi frekuensi, amplitudo dan pita suara setelah dilakukan proses enkripsi dan dekripsi data dengan algoritma Mars.
4. Mengetahui perbedaan ukuran file setelah dilakukan proses enkripsi dan dekripsi data.

1.4 Metodologi penyelesaian masalah

Metodologi penyelesaian masalah dalam penelitian Tugas akhir ini adalah:

1. Studi literatur dengan mempelajari buku-buku referensi dan mengumpulkan bahan-bahan online dari internet, seperti jurnal-jurnal, artikel-artikel dan paper untuk memperoleh pengertian dan pengetahuan tentang kriptografi, algoritma kriptografi MARS, enkripsi dan dekripsi data dan struktur file mp3.
2. Melakukan perancangan dan implementasi perangkat lunak untuk enkripsi dan dekripsi data dengan algoritma MARS dengan menganalisis permasalahan dan kebutuhan yang diperlukan untuk membangun perangkat lunak.
3. Melakukan pengujian sesuai parameter yang telah ditentukan dan membuat analisis dari hasil pengujian tersebut.
4. Membuat kesimpulan akhir berdasarkan analisis hasil pengujian dan menyusun laporan.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Dari hasil pengujian, dapat diambil kesimpulan sebagai berikut :

1. Proses enkripsi suatu file mp3 menyebabkan ukuran file tersebut bertambah sebesar 20 byte, hal ini disebabkan adanya penyimpanan bit hasil fungsi hash yang jumlahnya 160bit pada file hasil enkripsi.
2. Properti file yang meliputi frekuensi dan amplitudo akan kembali seperti semula setelah dilakukan proses dekripsi pada file terenkripsi. Hal ini dikarenakan tidak terjadi perubahan bit pada plainteks maupun cipherteks.
3. Waktu proses dekripsi lebih lama dibandingkan dengan proses enkripsi, hal ini disebabkan pada proses dekripsi terdapat proses pengecekan hasil fungsi hash.
4. Waktu proses enkripsi dan dekripsi data dengan algoritma Mars lebih lama dibandingkan dengan algoritma Twofish. Hal ini dikarenakan adanya perbedaan ukuran S-Box yang digunakan untuk membangun sistem. Pada algoritma Mars ukuran S-Box yang digunakan adalah 32 bit, sedangkan pada algoritma Twofish berukuran 8 bit.

5.2 Saran

Dalam implementasi algoritma Mars, sebaiknya panjang kunci yang digunakan tidak dibatasi hanya kunci 128 bit saja. Untuk pembangkitan sub kunci bisa juga digunakan fungsi hash yang lain, seperti Tiger, RIPEMD atau MD5.

Daftar Pustaka

[1] Burwick, Carolynn.,dkk.1999."*MARS-a candidate cipher for AES*". http://csrc.nist.gov/encryption/aes/round2/AESalgs/MARS/mars.pdf

[2] Galli, Retto**.** Winter 2000. *MARS Encryption Algoritm*. http://islab.oregonstate.edu/koc/ece575/00Project/Galli/MARSReport.html

[3] Halevi, Shai. 2000. *Key Agility in MARS*. http://www.ibm.com/security/key-agil.pdf

[4] IBM corp **.** *MARS – A Candidate cipher for AES.* http://www.tropsoft.com/strongenc/mars.pdf

[5] IBM MARS Team. 2000. *Comments on MARS's Linear Analysis.* http://www.ibm.com/security/liniear.pdf

[6] IBM MARS Team. 2000. *MARS and the AES Selection Criteri.* http://www.ibm.com/security/final-comments.pdf

[7] Lung, Chan., Rinaldi Munir. *Studi dan Implementasi Advanced Encryption Standard dengan Empat Mode Operasi Blok Cipher*. Bandung: Institut Teknologi Bandung.

[8] Kal-El.*The Story of AES (Advanced Encryption Standard)*

[9] Mean Opinion Score. "http://en.wikipedia.org/wiki/Mean_Opinion_Score".

[10] MP3 File Structure. "http://www.multiweb.cz/twoinches/mp3inside.htm"

[11] Munir, Renaldi. *Kriptografi*. Bandung: Informatika.