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.