BAB I
PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan merupakan salah satu aspek penting dari suatu sistem informasi. Salah satu cara pembatasan akses data bagi pihak-pihak yang tidak berhak yaitu dengan enkripsi. Enkripsi adalah proses mengkonversi pesan (*plaintext*) ke dalam bentuk *cryptogram* atau *ciphertext*. Proses ini dapat secara *software* atau *hardware* serta memerlukan *key* untuk menjalankan algoritma *Cipher* kemudian di deskripsi oleh sisi penerima dengan perangkat dan *key* yang bertipe sama, guna mendapatkan kembali *plaintext* semula.

Beberapa alasan pengguna enkripsi yaitu mencegah mereka yang tidak berwenang melihat data-data sensitif, mengurangi kemungkinan terbukanya data rahasia tanpa sengaja, mencegah mereka yang mempunyai akses istimewa agar tidak dapat melihat data pribadi dan untuk mempersulit usaha penyusup memasuki sistem.

Data yang akan dienkripsi pada tugas akhir ini adalah berupa audio digital yang tidak terkompresi. Audio digital yang akan diproses mempunyai tingkat kesulitan yang lebih kompleks dikarenakan dari ukuran matrik yang besar. Sehingga dibutuhkan metode enkripsi yang mampu menangani masalah tersebut dengan waktu proses yang cepat dan memiliki tingkat sekuritas yang tinggi terhadap serangan dari pihak yang tidak diinginkan.

Pada tugas akhir ini metode enkripsi yang digunakan adalah metode *chaotic-map*. Adapun metode *chaotic-map* yang digunakan adalah *Baker Map*. Algoritma Baker Map ini adalah algoritma yang cepat untuk citra karena kecepatannya inilah diusulkan untuk audio**.**[1] [2] Pada pengimplementasiannya metode ini akan dibandingkan dengan metode *DES*.

Dengan membandingkan kedua metode tersebut, diharapkan sistem dari metode *Baker Map* mampu melakukan proses enkripsi dengan waktu yang cepat dan tingkat sekuritas yang baik. Sehingga data yang dikirimkan akan tetap terjaga kerahasiannya sampai diterima oleh penerima tanpa diketahui oleh pihak luar.

1.2 Tujuan

Tujuan dari penulisan Tugas Akhir ini adalah :

- Mendesain dan mengimplementasikan enkripsi sinyal audio dengan menggunakan algoritma *Baker Map*.
- Menguji tingkat keamanan dan kecepatan proses dari metoda *Baker Map*.
- Menguji tingkat waktu komputasi terhadap fungsi dari variasi kunci.
- Menganalisa performansi dari sistem enkripsi dilihat dari kecepatan proses dan tingkat keamanannya.
- Membandingkan hasil analisis menggunakan metoda *Baker Map* dengan metoda enkripsi klasik *DES*.

1.3 Rumusan Masalah

Beberapa permasalahan pada tugas akhir dapat didefinisikan sebagai berikut :

1. Proses enkripsi sinyal audio membutuhkan suatu algoritma yang mampu mengatasi *file* dengan ukuran yang besar.

2. Algoritma *Baker Map* memiliki kelebihan dalam hal kecepatan dengan data yang berukuran besar.

1.4 Batasan Masalah

Agar pembahasan dalam Tugas Akhir ini tetap terarah pada tujuan pokoknya, maka perlu dilakukan beberapa pembatasan terhadap permasalahannya, yaitu :

1. Informasi yang akan dienkripsi adalah sinyal audio dengan format .*WAV*.
2. Algoritma enkripsi yang digunakan adalah *Baker Map*.
3. Lama waktu komputasi linier yang diujikan adalah 2 detik, 4 detik, 6 detik, 8 detik, 10 detik dan 12 detik.
4. Lama waktu komputasi geometri yang diujikan adalah 2 detik, 4 detik, 16 detik, 32 detik dan 64 detik.
5. Proses dari Algoritma Baker Map hanya menggunakan ukuran matrik 256 x 256, matrik 512 x 512 dan matrik 1024 x 1024.
6. Proses enkripsi menggunakan variasi kunci 2, 8, 16, 32, 64, dan acak.

7. Tidak memperhatikan proses pentransmisiannya dan diasumsikan tidak ada error pada saat transmisi data.
8. Simulasi dilakukan dengan menggunakan *software Matlab* 7.4.0.287 (R2007a).

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam pencapaian Tugas Akhir ini adalah :

1. Studi Literatur yang dilakukan untuk mempelajari konsep dasar dan teori pendukung yang berhubungan dengan permasalahan pada tugas akhir ini.
2. Pencarian data yang dilakukan sebagai bahan untuk proses analisa. Data yang digunakan adalah data berupa audio dengan *format .WAV*.
3. Merancang program simulasi pada software *Matlab* 7.4.0.287 (R2007a) yang akan digunakan untuk pengimplementasian proses enkripsi.
4. Menganalisa data yang telah didapat dengan program simulasi sesuai dengan parameter yang telah ditentukan.
5. Mengambil kesimpulan dari hasil analisa yang telah dilakukan dilihat dari parameter yang ada serta memberi saran untuk penelitian selanjutnya.

1.6 Sistematika Penulisan

BAB I Pendahuluan

Pada bab ini dijelaskan mengenai latar belakang, tujuan, rumusan masalah, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II Dasar Teori

Pada bab ini berisikan mengenai teori dasar enkripsi, input sistem dan teori dasar mengenai metode *Baker Map* yang digunakan pada sistem dan skema dari metode tersebut.

BAB III Perancangan Dan Implementasi Enkripsi Dengan *Baker Map*

Pada bab ini berisikan rancangan sistem dan simulasi sistem enkripsi dengan masukan audio dengan *format .WAV* dan kemudian dienkripsi menggunakan software *Matlab* 7.4.0.287 (R2007a).

BAB IV Hasil Analisa Simulasi

Bab ini berisi hasil penelitian dari hasil simulasi, perbandingan tingkat efisiensi performansi dari sistem enkripsi dan analisis statistik dari keluaran enkripsi.

BAB V Penutup

Pada bab ini akan di muat kesimpulan akhir dari analisis yang telah dilakukan pada bab IV, dan saran yang berkaitan dengan masalah yang dibahas untuk pengembangan penelitian ini.