BAB I
PENDAHULUAN

1.1 Latar Belakang

Kriptografi adalah ilmu yang mempelajari teknik-teknik yang berhubungan dengan aspek keamanan informasi. Pada kriptografi terdapat proses enkripsi dekripsi, yaitu proses penyandian dan pengembalian informasi. Kriptografi sendiri saat ini telah berkembang dengan pesat. Banyak algoritma yang bermunculan seperti DES, 3DES, IDEA, AES dan lain-lain. Kriptografi pun banyak diterapkan untuk mengamankan data digital yang dikirimkan melalui media transmisi. Data digital dapat berupa suara, gambar, video dan lain lain.

AES *(Advanced Encrytpion Standard)* adalah algoritma klasik yang bersifat simetris dan *cipherblock* serta beroperasi dengan mode *bitstream*. AES telah banyak diimplementasikan dalam berbagai aplikasi. Karena memiliki kelebihan kekuatan enkripsi yang sangat baik. Namun AES memiliki kelemahan dari sisi waktu enkripsi-dekripsi. Sehingga jika informasi yang disampaikan berupa citra digital seperti gambar, AES kurang cocok digunakan. Hal ini dikarenakan gambar memiliki ukuran yang lebih besar daripada data. Karena itu muncul berbagai teori sebagai dasar algoritma kriptografi baru. Salah satunya adalah teori *Chaos*.

Teori *Chaos* adalah teori yang menggambarkan kebiasaan dari suatu sistem yang terus berubah yang menyebabkan memiliki sifat untuk muncul secara acak. Beberapa contoh metode teori *Chaos* adalah *Arnold's Cat Map, Logistic Map, Henon Map* dan lain sebagainya. Dalam kriptografi, teori *Chaos* digunakan untuk membangkitkan bilangan secara acak, yang akan dimanfaatkan sebagai *keystream* dalam melakukan proses enkripsi atau untuk mengacak susunan *pixel* gambar. Penerapan teori *Chaos* dalam kriptografi telah menjadi topic yang banyak dibicarakan, karena sifat teori *Chaos* yang *sensitive* terhadap perubahan dari kondisi awal [1].

Beberapa penelitian pun sudah dilakukan untuk membandingan performansi algoritma AES dan algoritma berbasis teori *Chaos*. [2] telah membuktikan bahwa AES memiliki tingkat keamanan lebih baik dari pada *Logistic Map*. Dari sisi kecepatan enkripsi *Logistic Map* lebih baik daripada AES. Hal ini dikarenakan jika

metode teori *Chaos* yang digunakan untuk enkripsi hanya satu jenis, tingkat keamanan yang dihasilkan kurang begitu bagus. Oleh karena itu beberapa penelitian penggabungan metode teori *Chaos* muncul. Sedangkan [3] telah melakukan penelitian dengan menggunakan *Arnold's Cat Map* (ACM) untuk mengacak susunan *pixel* dan Logistic Map untuk mengubah nilai *pixel*. Hasil analisis menunjukkan *cipher image* tidak dapat dikenali dan nilai *pixel*-nya tidak saling berhubungan, namun kriptografi berbasis *Logistic Map* memiliki ruang kunci yang kecil dan keamanan yang lemah. Oleh karena itu muncul penelitian mengenai metode lain berbasis teori *Chaos*. [4], melakukan penelitian mengenai *Henon Map*. Dari hasil analisis yang dilakukan, diperoleh bahwa enkripsi dengan metode *henon map* memiliki ruang kunci yang besar dan keamanan yang tinggi.

Semakin berkembangnya teknologi informasi dan komunikasi, akan menuntut sistem keamanan ditingkatkan. Namun sistem keamanan yang dimaksud tidak hanya masalah keamanan nya yang diperhatikan, namun juga waktu proses pada sistem keamanan tersebut. Hal inilah yang mendasari dilakukan penelitian dengan membandingkan enkripsi gambar dengan menggunakan algoritma AES dan algoritma berbasis teori *Chaos*. Metode *Chaos* yang digunakan adalah *Arnold's Cat Map* dan *Henon Map.*

1.2 Rumusan Masalah

Berdasarkan pada latar belakang tersebut, rumusan masalah pada tugas akhir ini adalah :

a. Mengapa teori *Chaos* digunakan untuk teknik enkripsi citra digital ?
b. Bagaimanakah mekanisme enkripsi gambar dengan menggunakan algoritma berbasis teori *Chaos* ?
c. Bagaimanakah cara menggabungkan metode *Chaos Arnold's Cat Map* dengan *Henon Map* ?
d. Bagaimanakah perbandingan performansi algoritma AES dan algoritma berbasis teori *Chaos* untuk enkripsi gambar ?

1.3 Tujuan Penelitan

Tujuan dari pelaksanaan tugas akhir ini antara lain :

a. Melakukan simulasi algoritma berbasis teori *Chaos*

b. Mengetahui cara menggabungkan Arnold's Cat Map dan Henon Map
c. Mengetahui perbandingan performansi antara algoritma AES dan algoritma berbasis teori *Chaos*

1.4 Batasan Masalah

Batasan masalah pada tugas akhir ini adalah :

a. Simulasi menggunakan MATLAB
b. Hanya membahas untuk enkripsi gambar *greyscale*
c. Panjang kunci yang dipakai adalah 128 bit untuk AES
d. Parameter perbandingan performansi meliputi waktu proses enkripsi dan dekripsi, BER *(Bit Error Rate),* analisis histogram, analisis korelasi, analisis AWGN dan PSNR, *avalanche effect, brute force attack* dan nilai MOS *(Mean Opinion Score).*

1.5 Metode Penelitian

Metode yang dilakukan di dalam pelaksanaan tugas akhir ini sebagai berikut :

1. Studi literature

   Literatur dalam hal ini baik berupa buku, catatan, hasil penelitian, dan sumber-sumber elektronik di internet. Studi literatur ini ditujukan untuk mendapatkan referensi yang jelas dan tepat mengenai simulasi yang akan dibuat.

2. Implementasi sistem

   Melakukan implementasi terhadap algoritma AES dan AES berbasis teori *Chaos* menggunakan matlab.

3. Tahap uji dan analisis perbandingan

   Dilakukan analisis terhadap hasil yang didapatkan sehingga sesuai dengan harapan

4. Kesimpulan

   Pengambilan kesimpulan terhadap hasil analisis dan pembuatan laporan Tugas akhir dari seluruh kegiatan penelitian.

1.6 Sistematika Penelitian

Pada pelaksanaan tugas akhir ini terdapat lima bab utama serta lampiran yang bertujuan untuk menunjang kelengkapan informasi pada pelakasanaan tugas akhir ini. Adapun lima bab utama pada tugas akhir ini adalah :

BAB I PENDAHULUAN

Pada Bab ini berisi uraian secara singkat mengenai latar belakang permasalahan, perumusan masalah, tujuan penelitian, pembatasan masalah penelitian, metodologi penelitian, sistematika penulisan, dan waktu pelaksanaan penelitian

BAB II DASAR TEORI

Bab ini berisi tentang teori dasar mengenai kriptografi, algoritma AES, teori *Chaos*, serta teori dasar lain yang berkaitan dengn pelaksanaan tugas akhir ini.

BAB III PERANCANGAN SISTEM

Bab ini membahas mengenai blok diagram, flow chart, dan proses desain serta perancangan sistem enkripsi-dekripsi pesan teks menggunakan kedua algoritma tersebut.

BAB IV PENGUJIAN SISTEM DAN ANALISIS HASIL PERBANDINGAN

Bab ini membahas tentang analisis hasil sistem yang dijalankan. Analisis dilakukan terhadap perbandingan parameter kinerja sistem yang diamati saat setelah proses enkripsi-dekripsi dijalankan

BAB V PENUTUP

Bab ini berisi kesimpulan hasil simulasi dan analisis serta saran sebagai bentuk pengembangan perancangan yang lebih baik lagi