

BAB I

PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang permasalahan, perumusan masalah, tujuan dan manfaat, batasan masalah, dan sistematika penulisan dalam penelitian ini.

1.1. Latar Belakang

Semakin majunya perkembangan teknologi dan banyaknya persaingan ketat dalam bidang teknologi membuat developer aplikasi dipaksa untuk menemukan terobosan baru agar produknya terlihat lebih unggul dari pesaingnya, seperti contohnya pada zaman sekarang tengah ramai bermunculan aplikasi seperti Instagram, Whatsapp, Facebook dan aplikasi lain yang memanjakan penggunaanya dengan mudahnya mengirim pesan atau bertukar foto. Tak jarang pula beberapa oknum tak bertanggung jawab kadang mencari kelemahan untuk meretas dan mendapatkan data yang bersifat rahasia atau privasi. Sehingga dibuatlah sistem pengaman pada aplikasi tersebut, agar saat pengiriman data tidak dapat dibuka dengan mudah karena berbentuk file enkripsi. Teknik pengamanan data dengan enkripsi dan dekripsi pada citra dikenal sebagai kriptografi.

Kriptografi adalah ilmu atau seni yang menggunakan matematika untuk mengamankan suatu informasi. Pengamanan ini dilakukan dengan menjalankan algoritma enkripsi (mengubah informasi awal menjadi informasi baru yang disamarkan dengan menggunakan suatu kunci) dan dekripsi (mengubah kembali menjadi informasi awal).

Kriptografi menjadi solusi mengatasi ancaman keamanan data. Metode – metode kriptografi diantaranya *AES Rijndael (Advance Encryption Standard)*, dan *Serpent*. Tentunya tidak ada yang tahu mana metode yang lebih baik karena sebuah metode memiliki kelebihan dan kekurangan yang beragam. Berdasarkan uraian – uraian tersebut penulis mendapatkan ide untuk menganalisa dan membandingkan dua metode tersebut, dengan skripsi berjudul “Analisis Perbandingan Algoritma *AES Rijndael* dan *Serpent* Pada Citra Digital”.

1.2. Perumusan Masalah

1.2.1. Permasalahan

Berdasarkan latar belakang yang telah diuraikan tersebut, terdapat beberapa rumusan masalah diantaranya :

1. Seberapa baik kualitas Citra hasil enkripsi dekripsi algoritma *AES Rijndael* dan *Serpent* pada Citra *Digital*?
2. Seberapa baik performa kecepatan enkripsi dan dekripsi algoritma *AES Rijndael* dibandingkan dengan *Serpent* pada Citra *Digital*?
3. Seberapa aman metode enkripsi *AES Rijndael* dibandingkan dengan *Serpent* pada Citra *Digital*?

1.3. Tujuan Dan Manfaat

1.3.1. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk membuat aplikasi pembanding dengan enkripsi dekripsi algoritma *AES Rijndael* dan *Serpent* pada Citra *Digital*.

1.3.2. Manfaat Penelitian

Adapun manfaat yang akan diperoleh dari penelitian ini adalah untuk mengetahui perbandingan hasil algoritma *AES Rijndael* dan *Serpent*.

1.4. Batasan Masalah

Dalam pembuatan aplikasi tersebut diperlukan beberapa batasan masalah agar ruang lingkup tetap terjaga dan mempermudah dalam pembuatan maupun perancangan. Adapun batasan masalah tersebut seperti berikut :

1. Parameter yang digunakan untuk pembanding meliputi, *TIME*, *PSNR*, *NPCR* dan *UACI*.
2. Jenis ukuran kunci hanya menggunakan 128 bit.
3. Jenis file yang dapat dibaca adalah “Citra/Gambar”.
4. Jenis citra yang dihasilkan adalah *Gray Scale*.
5. Bahasa pemrograman yang digunakan adalah *Matlab Production Server R2015a*.

1.5. Sistematika Penulisan

Dalam penelitian ini, sistematika penulisan yang digunakan terbagi menjadi lima bab dengan susunan sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan dasar-dasar dari penulisan laporan tugas akhir, yang terdiri dari latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat, serta sistematika penulisan laporan tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab ini membahas teori-teori yang berhubungan dengan penelitian, meliputi batik Madura, promosi internet, media sosial, *twitter*, *social media optimization*, *paired t-test*, dan penelitian terkait.

BAB III METODE USULAN

Bab ini menjelaskan tentang studi literatur, rancangan sistem, dan pengujian yang akan dilakukan serta analisis kebutuhan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil dari metode yang didapatkan terhadap masalah yang ada, kemudian dilakukan uji coba dan evaluasi terhadap metode yang diimplementasikan pada web.

BAB V PENUTUP

Bab ini membahas kesimpulan yang diperoleh dari hasil penelitian serta saran-saran yang ditujukan bagi para pembaca dan pengembang sistem untuk penelitian selanjutnya.