BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi mengalami perkembangan yang pesat sehingga mampu menciptakan suatu hal yang dapat mendukung perkembangan informasi tersebut, salah satunya yaitu rumah sakit. Informasi tersebut saat ini dapat disajikan dan disimpan dalam bentuk digital dan memiliki beberapa bentuk seperti teks, video, audio, dan gambar. Gambar medis digital berperan penting dalam mendiagnosa dan mengobati penyakit. Secara umum, gambar medis mungkin melibatkan banyak privasi pasien dan sangat rahasia serta sensitif. Kecelakaan yang menghancurkan dapat terjadi jika gambar pribadi ini dicuri, dilihat, atau digunakan dengan akses yang tidak sah.

Untuk membatasi penyalahgunaan citra digital pasien oleh pihak tidak bertanggung jawab, salah satu solusinya yaitu mengamankan data tersebut dengan cara disamarkan sehingga tidak dapat dilihat maupun diakses. Citra digital (dokumen gambar) merupakan suatu data penting yang sering diabaikan dampak buruknya apabila disalahgunakan. Saat ini, sudah banyak teknologi yang dikembangkan untuk melindungi banyak jenis gambar seperti gambar medis. Di antara teknologi ini, enkripsi adalah cara paling efektif untuk mengubah gambar menjadi gambar yang tidak dikenali. Enkripsi adalah suatu proses mengubahsebuah teks murni *(plaintext*) menjadi sebuah runtutan karakter atau data yang terlihat berarti dan mempunyai urutan bit yang tidak beraturan, disebut *ciphertext*. Proses mengubah kembali *ciphertext* menjadi *plaintext* disebut dekripsi [1].

Terdapat banyak algoritma penyandian yang digunakan untuk mengamankan suatu data. Namun, algoritma yang cukup terkenal adalah algoritma RSA (*Rivest Shamir Adlement*). RSA merupakan suatu algoritma yang dibuat pada tahun 1977 yang diberi nama berdasarkan singkatan para penemunya, yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman [2]. Keamanan pada algoritma ini ditunjukkan dengan sulitnya mencari hasil faktor prima dari bilangan yang besar. Hasil pemfaktoran tersebut yang digunakan untuk memperoleh kunci private. Selama

belum ditemukan algoritma yang tepat untuk memfaktorkan bilangan yang besar menjadi faktor prima, maka selama itu pula keamanan algoritma RSA tetap terjaga.

Penelitian ini menggunakan teknik kriptografi sebagai pengamanan yang dapat menyamarkan gambar digital menggunakan metode RSA-CRT (*Rivest Shamir Adleman Chinese Remainder Theorem*). Metode RSA-CRT dipilih karena berdasarkan [3], RSA dapat digunakan untuk mengenkripsi suatu gambar [3]. Namun berdasarkan [4], metode RSA membutuhkan waktu lebih lama dalam proses dekripsi sehingga untuk mengatasi kelemahan tersebut ditambahkan teorema CRT untuk mempercepat proses Dekripsi tersebut [4]. Berdasarkan (Chenchen Zang, 2016), RSA berbasis CRT memiliki struktur yang lebih sederhana dan mudah untuk diimplementasikan. Kekuatan keamanan dalam enkripsi dan Dekripsinya sama dengan RSA biasa namun lebih efisien dan hemat waktu dalam komputasi [6]. Sehingga RSA-CRT dinilai dapat pula menjadi suatu pilihan algoritma yang dapat digunakan untuk mengamankan suatu citra digital.

Berdasarkan uraian diatas, penelitian ini dilakukan untuk membandingkan akses kecepatan waktu tingkat keamanan data atau tingkat ketahanan terhadap serangan berkas melalui hasil enkripsi dan dekripsi antara algoritma RSA dengan RSA-CRT, sehingga diperoleh algoritma manakah yang lebih baik dalam melindungi data penting seperti citra digital pasien.

1.2 Rumusan Masalah

Rumusan masalah pada Tugas Akhir ini diantaranya:

1. Bagaimana cara suatu aplikasi untuk mengimplementasikan sistem kriptografi dalam mengamankan file gambar dengan menggunakan algoritma RSA dengan RSA-CRT.
2. Bagaimana penerapan metode RSA dengan RSA-CRT dalam proses enkripsi dan dekripsi file gambar.
3. Bagaimana evaluasi perbandingan pengujian algoritma RSA dengan RSA-CRT.

4. Apakah berkas yang telah dienkripsi dapat dikembalikan kembali menjadi bentuk berkas yang utuh seperti sebelum dilakukan proses enkripsi tanpa ada cacat sedikitpun.

1.3 Tujuan dan Manfaat

Tujuan dari penelitian ini adalah untuk melakukan perbandingan antara RSA dan RSA-CRT dalam akses kecepatan waku tingkat keamanan datanya atau tingkat ketahanan terhadap serangan berkas. Sedangkan manfaat yang diharapkan dari penelitian ini yaitu dapat mengetahui seperti apa penerapan metode RSA dan RSA-CRT dalam proses enkripsi dan Dekripsi suatu data citra digital. Selain itu dapat membandingkan hasil kedua algoritma yang telah melalui pengujian sehingga dapat dijadikan bahan pertimbangan dan rujukan dalam memilih metode untuk mengamankan suatu citra digital.

1.4 Batasan Masalah

Agar tidak terjadi kesalahan dalam persepsi dalam penelitian ini, maka dijelaskan batasan masalah pada laporan ini,

1. Berkas yang digunakan adalah berkas gambar dan berkas tersebut dapat diubah menjadi sebuah berkas baru yang tidak dapat dikenali berkas sebenarnya.
2. Pengolahan gambar hanya dilakukan pada citra skala RGB.
3. Aplikasi pengolahan citra digital menggunakan teknik kriptografi yaitu proses enkripsi dan Dekripsi.
4. Proses enkripsi dan Dekripsi menggunakan Algoritma RSA dan RSA-CRT.
5. Aplikasi ini merupakan aplikasi desktop yang berjalan pada sistem Operasi Windows.
6. Pemodelan data pada penelitian ini menggunakan pemodelan terstruktur.
7. Menggunakan bahasa pemrograman C# dengan aplikasi *Visual Studio 2019.*

1.5 Metode Penelitian

Adapun metode penelitian yang digunakan untuk merealisasikan tujuan dan perumusan masalah pada Tugas Akhir ini adalah sebagai berikut:

1. Studi Pustaka

   Pada tahap ini merupakan rangkaian pengumpulan untuk Pustaka acuan yang berhubungan dengan penelitian. Tahapan ini untuk mendapatkan informasi dan data mengenai file citra, metode RSA dan RSA-CRT. Referensi yang digunakan berupa buku, jurnal, skripsi yang berkaitan dengan penelitian ini.

2. Analisis dan Perancangan

   Tahap ini digunakan untuk mengolah data dari hasil studi Pustaka yang kemudian dilakukan analisis – analisis terhadap apa saja yang dibutuhkan dalam penelitian dan perancangan menggunakan algoritma RSA dan RSA-CRT sehingga menjadi suatu aplikasi dengan susunan yang jelas.

3. Implementasi

   Pada tahap ini, membuat sebuah aplikasi dengan menggunakan Bahasa pemrograman sesuai dengan diagram yang telah dirancang.

4. Pengujian

   pada tahap ini, menguji apakah aplikasi yang dibuat telah berhasil berjalan sesuai dengan kebutuhan yang ditentukan sebelumnya dan melakukan koreksi bila masih diperoleh *error* pada aplikasi.

5. Dokumentasi

   Pada tahap ini, penelitian melakukan dokumentasi dan penulisan laporan dan kesimpulan akhir dari hasil akhir Analisa dan pengujian dalam bentuk Tugas Akhir mengenai program tersebut yang bertujuan untuk menunjukkan hasil penelitian ini.

1.6 Sistematika Penulisan

Berikut adalah sistematika dalam penulisan Tugas Akhir yang terbagi menjadi lima (5) bab, yaitu:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang masalah, rumusan masalah, tujuan dan manfaat, Batasan masalah, metode penelitian, serta sistematika penulisan.

BAB II KONSEP DASAR

Bab ini berisi tentang dasar teori yang mendukung atau berkaitan dengan Tugas Akhir ini, yaitu yang terdiri dari enam (6) subbab dengan bahasan teori yang mendasar dan rinci.

BAB III PERANCANGAN SISTEM

Bab ini menjelaskan alur percobaan secara garis besar disertai dengan proses desain aplikasi yang digunakan.

BAB IV HASIL DAN ANALISIS

Bab ini membahas mengenai hasil dari percobaan yang dilakukan dan analisis terhadap hasil tersebut.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari hasil percobaan aplikasi yang dibuat pada Tugas Akhir ini dan saran untuk penelitian selanjutnya.