BAB I
PENDAHULUAN

1.1 Latar Belakang

Pengamanan berupa data adalah hal yang sangat sensitif dalam menjaga sebuah kerahasiaan data ataupun informasi, terutama yang berisi data ataupun informasi yang sangat penting dan hanya boleh diketahui oleh orang tertentu, sehingga perlu dilakukan sebuah pengamanan data ganda supaya pihak yang tidak memiliki kepentingan tidak bisa membuka ataupun mengetahui informasi yang dikirimnya. Salah satu cara untuk menjaga keamanan kerahasiaan pada suatu data maupun informasi yaitu dengan teknik *kriptografi*.

Penggunaan informasi berupa gambar sudah sering dipergunakan dari jaman dahulu. Bahkan dalam kehidupan pun sangat erat hubungannya dengan media berupa file gambar. Akan tetapi, penggunaan media informasi melalui gambar memiliki beberapa kelemahan. Kelemahan tersebut adalah mudahnya file berupa gambar tersebut dirubah oleh pihak yang tidak memiliki kepentingan. Terlebih lagi jika informasi itu berupa file gambar tersebut mempunyai sifat rahasia. Dari sinilah mengapa tingkat keamanan menggunakan media gambar telah menjadi topik penting dalam dunia digital. Apalagi pada akhir-akhir ini jumlah kejahatan di bidang teknologi informasi telah meningkat pesat pada saat ini (Chin, 2001).

Dalam hal menjaga sebuah kerahasiaan informasi data berupa file gambar maka memerlukan teknik – teknik dekripsi maupun enkripsi yang tidak mudah dipecahkan. Dalam proses pengamanan file berupa gambar tersebut menggunakan beberapa metode algoritma tertentu yang dapat memberikan pengamanan ganda terhadap data maupun informasi berupa file tersebut agar dengan tidak bisa di baca maupun dimengerti oleh pihak lain. Salah satunya dengan metode algoritma Ron Rivest, Adi Shamir, dan Leonard Adleman (RSA). Dalam beberapa penelitian terdahulu mengenai implementasi algoritma RSA. Algoritma RSA dapat di aplikasikan untuk berbagai jenis enkripsi

dekripsi, pesan teks, email, maupun pesan gambar (Pratama, 2016). Namun dalam kesimpulan penelitian tersebut didapatkan hasil bahwa bisa saja sewaktu-waktu file tersebut dimanipulasi oleh beberapa pihak yang tidak berwenang. Penelitian sebelumnya mengenai algoritma RSA untuk sebuah keamanan data yang dilakukan oleh (Utara, 2003) yaitu Studi Dan Implementasi Keamanan Data Dengan Tanda Tangan Digital. Hasil yang didapatkan dalam penelitian diatas ialah tanda tangan digital dapat dibangun dengan cara menerapkan algoritma RSA. Hasil pengujian menunjukkan bahwasannya tanda tangan digital tersebut dapat mengidentifikasikan pesan yang ditandatanganinya, sehingga pesan tidakr dapat dipalsukan maupun diubah tanpa dengan diketahui. Perangkat lunak tersebut dapat mensimulasikan tujuan tanda tangan digital tersebut meliputi integritas data dan otentitikasi. Inputan bilangan prima dalam suatu pembangkitan kunci dapat dikembangkan menjadi inputan data yang berupa teks dan selanjutnya akan dirubah menjadi bilangan prima, sehingga inputan sangat mudah dilakukannya tanpa harus mengetahui bilangan prima.

Penelitian yang akan dilakukan adalah dengan mengkombinasikan metode RSA dengan metode DSA (*Digital Signature Algoritem*). Pemilihan metode algoritma Ron Rivest, Adi Shamir, dan Leonard Adleman (RSA) dipilih karena algoritma RSA merupakan salah satu algoritma enkripsi terkuat saat ini, dan lebih baik dibanding DSA ataupun SED. Algoritma RSA juga berisi pemfaktoran yang sangat rumit sehingga tidak dengan mudah dibobololeh orang lain. Metode DSA ditambahkan di dalam penelitian ini dikarenakan metode DSA memiliki hasil yaitu dalam aplikasi tanda tangan digital yang menggunakan algoritma kriptografi RSA dapat menjamin keamanan dokumen yang ditandatanganinya dalam beberapa aspek yaitu *integrity*, *authentication*, dan *non-repudiation* (Anshori, Erwin Dodu, & Wedananta, 2019).

1.2 Rumusan Masalah

Adapun perumusan masalah daripada penelitian ini yaitu :

"Bagaimana cara menerapkan metode tanda tangan digital dan Algoritma RSA dalam hal pengamanan data file berupa gambar ?".

1.3 . Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengetahui penerapan metode *Digital Signature* dengan Algoritma RSA dalam proses pengamanan file berupa gambar.
2. Memberikan pengamanan terhadap data file berupa gambar.

1.4 Manfaat Penelitian

Manfaat dari penelitian skripsi ini adalah untuk mencegah terjadinya pencurian maupun manipulasi file data berupa gambar oleh pihak yang tidak berwenang.

1.5 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah:

1. Data berupa gambar yang digunakan adalah data gambar dengan ekstensi PNG.
2. Pada penelitian ini nilai p dan q yang akan digunakan dibatasi dengan rentang 2 – 99.

1.6 Metodologi Penelitian

Pada penelitian kali ini metode yang digunakan adalah sebagai berikut.

1. Studi Pustaka

   Penulis melakukan studi pustaka dengan mempelajari berbagai buku – buku referensi maupun dari sumber – sumber yang ada kaitannya dengan penelitian ini, baik dari buku, jurnal maupun internet yang membahas tentang kriptografi,pengamanan data, maupun metode RSA maupun *Digital Signature*.
2. Analisis sistem

Pada tahap analisis sistem ini penulis diharapkan dapat memenuhi kebutuhan yang diharapkan oleh pengguna dengan berdasarkan hasil observasi dan pengumpulan data yang dilakukan. Analisa kebutuhan sistem juga dapat dilakukan untuk menentukan fitur apa saja yang terdapat pada sistem yang dibuat.

3. Perancangan

   Pada tahap perancangan, penulis memberikan sebuah gambaran secara lengkap tentang konsep yang akan diterapkan dalam pembuatan sistem.

4. Implementasi

   Pada tahap implementasi meliputi tahap pembuatan sistem kriptografi pengamanan data. Konsep yang sudah ada pada tahap penelitian sebelumnya akan di terapkan berdasarkan rancangan yang telah dibuat sebelumnya.

5. Pengujian

   Pada tahap ini dilakukan pengujian terhadap sistem yang dibuat untuk mengetahui apakah sistem tersebut bekerja sesuai dengan yang diharapakan.

1.7 Sistematika Penulisan

Dalam mempermudah penulisan laporan penelitian kali ini, maka sistematika penulisan yang digunakan adalah sebagai berikut :

BAB I : PENDAHULUAN

Bab pendahuluan ini menjelaskan mengenai latar belakang masalah, rumusan masalah , batasan masalah tujuan, penelitian, manfaat penelitian, sistematika penulisan,metodologi penelitian dan.

BAB II : LANDASAN TEORI

Bab ini akan membahas tentang teori – teori yang berhubungan dengan kriptografi, pengamanan data, Metode RSA,Metode DSA, file data gambar.

BAB III : ANALISA DAN PERANCANGAN SISTEM

Bab ini akan membahas tentang analis data yang akan diolah dalam sistem kriptografi serta membuat perancangan sistem pengamanan data yang akan dibuat.

BAB IV : IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini akan menjelaskan tentang bentuk sistem kriptografi pengamanan data berupa file gambar menggunakan Metode DSA RSA.

BAB V : PENUTUP

Bab terakhir memuat tentang kesimpulan semua isi dari keseluruhan uraian bab sebelumnya dan saran dari hasil yang didapatkan serta diharapkan dapat berguna dalam pengembangan selanjutnya.