BAB I
PENDAHULUAN

1.1 Latar Belakang

Berkembangnya teknologi informasi, tidak lepas dari permasalahan keamanannya. Oleh karena itu, dikembangkan metode - metode kriptografi file yang digunakan sebelum file dikirimkan atau diberikan kepada orang yang dituju. Kriptografi pada masa sekarang memiliki berbagai masalah. Salah satu masalah dasar yang masih terjadi adalah menjamin keamanan komunikasi di media yang tidak aman (Bellare, 2005). Hal di atas menyebabkan sebuah masalah muncul dari penyebaran file tentang integritas dari file tersebut.

Kriptografi adalah ilmu mengenai teknik enkripsi di mana input data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali input data asli (Kromodimoeljo, 2010). Enkripsi bertujuan untuk melakukan proses pengacakan pada isi input data yang asli. Di mana input data yang dipakai dalam penelitian ini berupa file. Proses pengacakan untuk mengubah file asli menjadi file acak. Isi dari file acak ini sulit untuk dibaca oleh orang yang tidak berhak mengakses berkas file tersebut, karena orang tersebut tidak memiliki kunci dekripsi. Makna “sulit untuk dibaca” di sini adalah probabilitas mendapatkan kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi adalah sangat kecil (Kromodimoeljo, 2010). Dengan menggunakan proses enkripsi dan dekripsi, kriptografi memiliki kemampuan untuk memberikan perlindungan dari serangan *hacker* atau *cracker* kepada file.

File diberi perlindungan dengan dienkripsi, sehingga bentuk asli file ini hanya dapat diubah atau didapatkan ketika didekripsi oleh pihak penerima.

Dengan *digital signature*, maka integritas data dapat dijamin, disamping itu juga digunakan untuk membuktikan asal pesan (keabsahan pengirim dan anti penyanggahan). Hanya sistem kriptografi kunci publik yang cocok dan alami untuk pemberian *digital signature*. Hal ini disebabkan karena *digital signature* berbasis kriptografi kunci publik dapat menyelesaikan masalah penyangkalan seseorang ketika transaksi atau *non-repudiation* (baik penerima dan pengirim pesan mempunyai pasangan kunci masing-masing) (Munir, 2006). Algoritma kriptografi kunci publik yang digunakan pada penelitian ini adalah *Rivest-Shamir-Adleman* (RSA). Selain algoritma kriptografi kunci publik, *digital signature* juga menggunakan algoritma SHA256 untuk proses pembuatan *hash value* atau *hashing*.

Algoritma kunci simetrik mampu membuat proses enkripsi dekripsi lebih kuat (Yadav, 2010). Untuk memperkuat *ciphertext* yang dihasilkan oleh algoritma RSA, penulis menambahkan satu algoritma kunci simetrik untuk proses enkripsi dekripsi yaitu algoritma *twofish*.

Dalam ilmu kriptografi masih banyak terdapat metode yang dapat digunakan untuk mengamankan file. Setiap metode memiliki kelebihan dan kekurangannya masing – masing. Tetapi yang menjadi kendala adalah mengetahui dan memahami cara kerja dari metode kriptografi tersebut (Dahria, 2012). Oleh karena itu, diperlukan sebuah perangkat lunak untuk mempelajari metode - metode tersebut.

Berdasarkan latar belakang yang sudah dijelaskan di atas, maka penulis memilih metode *digital signature* dan *twofish* untuk digabungkan ke dalam satu aplikasi sebagai sarana untuk membantu pembelajaran mengenai metode – metode kriptografi. Penulis juga melakukan penelitian *throughput* dari proses *hashing* dan enkripsi dekripsi dari ketiga algoritma.

1.2 Perumusan Masalah

Sesuai dengan latar belakang di atas, maka dapat dirumuskan permasalahan dalam skripsi ini sebagai berikut

Bagaimanakah waktu dan memori yang dibutuhkan proses enkripsi dan dekripsi dari algoritma RSA dan Twofish dengan menggunakan konsep *digital signature* pada aplikasi berkas pengaman digital?

1.3 Pembatasan Masalah

Pembatasan masalah penting untuk memfokuskan penelitian. Batasan masalah penelitian ini sebagai berikut

1.3.1 Algoritma diprogram pada bahasa pemrograman C# dengan menggunakan perangkat lunak Visual Studio 2010 sebagai IDE.

1.3.2 Enkripsi dekripsi menggunakan algoritma kriptografi RSA dan *Twofish*.

1.3.3 Pembuatan tanda tangan digital menggunakan algoritma *hashing* SHA256.

1.3.4 Penelitian tidak meliputi pembahasan aspek keamanan pada jalur komunikasi melalui internet yaitu prose transmisi file melalui jaringan internet.

1.3.5 Pengamanan berkas digital hanya meliputi enkripsi dekripsi terhadap file yang telah ditandatangani, autentikasi terhadap keaslian berkas digital sebagai hasil verifikasi pada saat file diterima.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah membangun aplikasi alat bantu pembelajaran untuk memahami pengamanan file dengan menggabungkan metode SHA256, *Rivest-Shamir-Adleman* (RSA) dan *Twofish*.

1.5 Manfaat Penelitian

Penelitian ini menghasilkan aplikasi yang dapat digunakan untuk alat bantu pratikum pembelajaran keamanan pada teknologi informasi dan sarana bagi penulis untuk mendapatkan pengalaman dalam mengembangkan sebuah aplikasi.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini menjelaskan tentang latar belakang permasalahan, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan tentang penjelasan singkat setiap bab.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai teori-teori dari sistem dan metode yang digunakan sebagai dasar teori untuk merancangn dan membangun aplikasi ini.

BAB III METODE PENELITIAN

Bab ini menjelaskan tentang metode penelitian yang mendukung dalam perancangan sistem, *flowchart*, dan perancangan *user interface*.

BAB IV IMPLEMENTASI DAN EVALUASI

Bab ini menjelaskan mengenai pembahasan secara detail mengenai implementasi sistem *digital signature* ke dalam aplikasi berkas pengaman digital dan analisis terhadap aplikasi itu sendiri.

BAB V KESIMPULAN

Bab ini berisi kesimpulan dari hasil proses aplikasi yang telah dibangun dan uji coba dari aplikasi berkas pengaman digital yang telah selesai.