BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kemudahan dalam pengiriman *file* secara elektronik memberikan sebuah celah keamanan, terutama jika *file* tersebut merupakan file yang sifatnya rahasia. Rahasia disini adalah sesuatu yang diketahui oleh sedikit orang atau terbatas. Khususnya kasus yang dialami perusahaan konsultan **Witdia Solusi Indonesia *Consultant*** atau disingat **WIS** dalam pengiriman *file*. Oleh karna itu perlu dilakukan pengamanan terhadap file yang dikirim melalui media *online.*

Keamanan *file* dapat dilakukan dengan metode kriptografi. Kriptografi itu sendiri adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan menyandingkan kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Untuk pengamanan *file* tersebut, perlu diperhatikan beberapa aspek-aspek agar *file* tersebut benar-benar asli dan tidak ada ubahan dari pihak lainnya.

Perusahaan ini mempunyai beberapa *point* yang dibuat menjadi file pdf. Didalam file tersebut memiliki *point-point* penawaran harga dan penawaran usulan teknis. *Point-point* tersebut yang akan dikirim kepada *user* sebagai bahan untuk mengambil suatu *tender* yang akan dikerjakan. Menurut **WSI** *point-point* tersebut rahasia, karena hanya pihak WSI dan *user* saja yang berhak tahu sampai antara kedua pihak *deal* akan perjanjian yang disepakati. Oleh karena itu dibutuhkan suatu pengamanan *file* untuk memberi rasa aman antar kedua belah pihak.

Solusi untuk meningkatkan rasa aman dalam pengiriman *file* melalui *online* yaitu menyisipkan suatu kriptografi sebagai Algoritma pengamanan *file* dengan memanfaatkan tanda tangan digital Algoritma atau *Digital Signature Algorithm* (DSA). Dengan memanfaatkan DSA, keamanan menjadi berlapis dan prinsip kriptografi yaitu menjaga kerahasiaan, integritas data, autentikasi dan menjaga entitas dapat dijalankan.

Dengan latar belakang yang dijelaskan diatas, maka penulis mencoba membuat suatu aplikasi pengamanan dengan menggunakan metode Algoritma

DSA untuk mengefektifkan pengamanan *file*. Berharap dengan menggunakan Algoritma DSA akan memperoleh aplikasi pengamanan. Sehingga dalam penelitian ini mengusulkan Algoritma DSA sebagai kriptografi untuk mengamankan *file*, oleh karena itu penelitian ini mengambil judul **"Pengamanan File Menggunakan Algoritma *Digital Signature Algorithm* (Studi Kasus : Witdia Solusi Indonesia)"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan diatas, terdapat rumusan masalah, yaitu:

Apakah sistem dapat mengamankan *file tender* dengan format pdf?

1.3 Tujuan Penelitian

Berdasarkan latar belakang, rumusan masalah dan ruang lingkup maka penelitian ini adalah untuk menghasilkan aplikasi pengamanan *file*.

a. Mengamankan *file* tender yang akan dikirim melalui media elektronik.
b. Mencegah pihak yang tidak bersangkutan mengetahui isi dari tender tersebut.

1.4 Manfaat

Berdasarkan dengan permasalahan dan tujuan penelitian yang telah disebutkan diatas, maka manfaat penelitian dapat dirumuskan sebagai berikut:

a. Dapat dijadikan sebagai bahan referensi terhadap penelitian tentang kriptografi menggunakan algoritma DSA..
b. Dapat meningkatkan sistem keamanan dan menjaga kerahasiaan *file* tender dalam pengiriman *file* tender dengan aman.
c. Melihat hasil ukuran *file* dari *file tender* sebelum maupun sesudah ter-enkripsi dan sebelum maupun sesudah ter-dekripsi.

1.5 Ruang Lingkup

Agar pembahasan skripsi ini dapat berjalan optimal, maka penulis membatasi pembahasan sebagai berikut:

a. Sistem dibangun dengan berbasis *WEB Server.*
b. Menggunakan kriptografi algoritma DSA kedalam sistem.
c. DSA digunakan sebagai sarana enkrip dan dekrip *file tender* dengan format pdf dengan ukuran maksimal 2.000 kilobyte.

1.6 Luaran Yang Diharapkan

Luaran yang diharapkan dalam penelitian ini adalah menghasilkan sebuah *prototype* aplikasi pengamanan *file* tender menggunakan algoritma DSA.

1.7 Sistematika Penulisan

Penulis akan memberikan gambaran mengenai isi dari penulisan laporan peneletian ini, sistematika penulisannya terdiri dari beberapa bagian utama sebagai berikut :

BAB 1 Pendahuluan

Bab ini menjelaskan mengenai latar belakang permasalahan, maksud dan tujuan, batasan masalah, waktu dan tempat penelitian, metode penelitian, serta sistematika penulisan.

BAB 2 Tinjauan Pustaka

Bab ini menjelaskan mengenai teori-teori sebagai acuan dalam penulisan laporan penelitian yang mendukung tema dan judul dari kegiatan yang dilakukan oleh penulis.

BAB 3 Tinjauan Umum

Bab ini menjelaskan tentang metode yang akan digunakan untuk membuat penelitian, kerangka kerangka berpikir, dan jadwal kegiatan.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini terdiri atas analisa permasalahan tentang semua hal terkait pengumpulan data yang diperlukan dalam perancangan sistem informasi akademik menggunakan DSA. Analisa perancangan aplikasi dan pembahasan berisikan tentang ide-ide penulis yang dituangkan dalam suatu rancangan aplikasi untuk memecahkan suatu masalah yang ada.

BAB 5 PENUTUP

Bab ini menjelaskan kesimpulan yang didapat dari hasi penelitian dan saran guna proses pengembangan selanjutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN