BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi memberi pengaruh besar bagi segala aspek kehidupan. Begitu banyak manfaat yang dapat diimplementasikan dalam kehidupan. Teknologi saat ini telah memberikan kemudahan dalam penyampaian suatu informasi. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko jika informasi yang sensitif dan berharga diakses oleh orang-orang yang tidak berhak. Aspek keamanan data sebenarnya meliputi banyak hal yang saling berkaitan, tetapi salah satu yang paling dikenal adalah sistem autentikasi.

Autentikasi berguna untuk menjaga agar suatu aksi hanya dapat dilakukan oleh aktor yang sudah memiliki hak akses. Salah satu jenis autentikasi yang paling dikenal adalah sistem *login* yang berupa *username* dan *password*. Jika *username* dan *password* tersebut diketahui orang lain maka sistem menjadi tidak aman.

Universitas Swadaya Gunung Jati Cirebon (Unswagati) memiliki *website* lokal yang sering diakses oleh para civitas akademika seperti sistem informasi dosen, sistem informasi mahasiswa, dan lain-lain. Sistem informasi tersebut memiliki autentikasi tersendiri bagi para penggunanya untuk menjaga hak akses tiap-tiap level pengguna. Sistem informasi tersebut menggunakan s*ecure socket layer* (SSL) sebagai jalur yang aman untuk pertukaran datanya. Tetapi SSL dapat di serang dengan menggunakan *tools* tertentu. Oleh karena itu maka perlu adanya sistem keamanan di dalam SSL itu sendiri.

Salah satu cara untuk mengamankan sistem adalah dengan menggunakan enkripsi. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Enkripsi data berfungsi untuk mengacak isi dari data atau *privacy* pada data, sehingga informasi yang ditransfer tidak mudah dikenali oleh pihak manapun. Hanya orang yang memiliki kunci untuk dekripsi pesan tersebut yang dapat membacanya.

Laporan penelitian ini diharapkan dapat membantu untuk mengamankan sistem autentikasi *website* khususnya sistem informasi siswa sehingga user dapat melakukan *login* dengan aman tanpa khawatir identitas dapat dicuri.

1.2 Rumusan Masalah

Dari latar belakang di atas maka masalah yang diteliti, dirumuskan sebagai berikut:

1 Bagaimana menerapkan algoritma RSA (Rivest-Shamir-Adleman) pada pengujian di sistem informasi mahasiswa Unswagati Cirebon untuk mengamankan sistem autentikasi ?

2 Bagaimana membuat enkripsi dengan algoritma RSA di sisi client dan dekripsi di sisi server?

1.3 Batasan Masalah

Adapun batasan-batasan masalah dalam laporan penelitian ini adalah sebagai berikut :

1. Laporan penelitian hanya terfokus pada implementasi algoritma RSA pada sistem informasi mahasiswa untuk sistem autentikasinya.
2. Implementasi yang dilakukan hanya pada jaringan lokal.
3. Elemen sistem autentikasi yang dienkripsi hanya *username* dan *password.*
4. Implementasi yang dilakukan hanya menggunakan Sistem Operasi Windows XP SP2 dengan *client* Windows XP SP2 karena dalam laporan penelitian ini tidak membahas mengenai keamanan *server*.

1.4 Tujuan

Tujuan dari laporan penelitian ini adalah:

1. Menguji sistem informasi autentikasi mahasiswa di Unswagati Cirebon dengan menggunakan algoritma RSA (Rivest-Shamir-Adleman) pada protokol SSL.
2. Membuat enkripsi dengan algoritma RSA di sisi *client* dan dekripsi di sisi *server*.

1.5 Sistematika Pembahasan

Sistematika pembahasan pada laporan penelitian ini dibagi menjadi beberapa bab yang meliputi:

BAB I PENDAHULUAN

Pada bab ini membahas mengenai latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan dan metode penelitian dari kegiatan penelitian laporan penelitian ini.

BAB II LANDASAN TEORI

Pada bab ini dibahas mengenai teori dasar yang digunakan pada penyusunan laporan penelitian yang meliputi penjelasan mengenai algoritma RSA, SSL, dan *web server*

BAB III ANALISIS DAN DISAIN

Pada bab ini dibahas mengenai perancangan model untuk konfigurasi sistem autentikasi yang kemudian diimplementasikan berbagai skenario yang digunakan untuk mendapatkan data yang diharapkan agar dapat dianalisis lebih lanjut.

BAB IV PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini dibahas mengenai analisa data-data yang telah diperoleh dari analisis sistem di jaringan yang kemudian menjadi bahan untuk pengembangan perangkat lunak.

BAB V TESTING DAN EVALUASI SISTEM

Pada bab ini berisi hasil testing dan evaluasi dari aplikasi perangkat lunak yang telah dibuat kemudian membandingkan dengan aplikasi yang selama ini sudah berjalan.

BAB VI KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dan saran dari seluruh kegiatan penelitian laporan penelitian ini yang dapat digunakan sebagai masukan untuk pengembangan sistem enkripsi RSA dan penelitian lebih lanjut.