BAB I
PENDAHULUAN

I.1 Latar Belakang

Kemajuan di bidang teknologi informasi telah memungkinkan institusi-institusi pendidikan atau lainnya melakukan interaksi dengan konsumen melalui jaringan komputer. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak. Aspek keamanan data sebenarnya meliputi banyak hal yang saling berkaitan, tetapi salah satu yang paling dikenal adalah masalah autentikasi.

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

Politeknik Telkom memiliki *website* lokal yang sering diakses oleh para civitas akademika seperti portal dosen, portal BAA, portal mahasiswa, dll. Portal-portal tersebut memiliki autentikasi tersendiri bagi para penggunanya untuk menjaga hak akses tiap-tiap level pengguna. Sampai saat ini *website* yang memiliki sistem keamanan adalah sisfo.politekniktelkom.ac.id. *Website* tersebut menggunakan SSL sebagai jalur yang aman untuk pertukaran datanya. Tetapi SSL sendiri dapat dijebol dengan menggunakan SSL strip. Oleh karena itu maka perlu adanya sistem keamanan di dalam SSL itu sendiri.

Salah satu cara untuk mengamankan sistem adalah dengan menggunakan enkripsi. Enkripsi dapat mengubah data mejadi bentuk lain yang tidak dapat dimengerti oleh orang lain. Walaupun orang lain dapat menjebol SSL dan

mendapatkan data yang lewat pada jaringan, dengan adanya enkripsi pada data maka data tersebut tidak dapat dibaca oleh orang tersebut. Hanya orang yang memiliki kunci untuk dekripsi pesan tersebut yang dapat membacanya.

Tugas akhir ini diharapkan dapat membantu untuk mengamankan sistem autentikasi *website* khususnya portal mahasiswa(students.politekniktelkom.ac.id) sehingga user dapat melakukan *login* dengan aman tanpa khawatir identitas mereka dicuri.

I.2 Rumusan masalah

Terdapat beberapa rumusan masalah yang akan di bahas dalam Tugas Akhir ini, yaitu sebagai berikut.

1 Bagaimana menerapkan algoritma RSA (Rivest-Shamir-Adleman) pada protocol SSL di portal mahasiswa di Politeknik Telkom untuk mengamankan sistem autentikasi ?

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

3 Bagaimana perbandingan tingkat keamanan antara portal mahasiswa Politeknik Telkom dan portal mahasiswa dalam tugas akhir ini?

4 Bagaimana menerapkan fungsi *hash* MD5 pada penyimpanan data autentikasi di *database*?

I.3 Batasan Masalah

Adapun batasan-batasan masalah dalam Tugas Akhir ini adalah sebagai berikut.

1. Tugas Akhir ini hanya terfokus pada implementasi algoritma RSA pada portal 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 Vista Home Premium dengan client Windows XP SP2 karena dalam tugas akhir ini tidak membahas mengenai keamanan server.
5. Adapun penggunaan tools yang digunakan dalam implementasi Tugas Akhir ini yaitu, *wireshark, Apache with mod* SSL sebagai webserver, *MySQL* sebagai *database*, dan *Open*SSL *0.9.8.*

I.4 Tujuan

Tujuan dari tugas akhir ini adalah:

1. Membuat sistem pengamanan autentikasi portal mahasiswa di politeknik telkom menggunakan algoritma RSA (Rivest-Shamir-Adleman) pada protocol SSL .
2. Membuat enkripsi dengan algoritma RSA di sisi client dan dekripsi di sisi server.
3. Membandingkan tingkat keamanan portal mahasiswa Politeknik Telkom saat ini dengan portal mahasiswa dalam tugas akhir ini.
4. Menerapkan fungsi *hash* MD5 dalam penyimpanan data autentikasi di *database*.

I.5 Sistematika Pembahasan

Sistematika pembahasan pada tugas akhir 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 tugas akhir ini.

BAB II LANDASAN TEORI

Pada bab ini dibahas mengenai teori dasar yang digunakan pada penyusunan tugas akhir yang meliputi penjelasan mengenai *Algoritma* RSA, MD5, 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 tugas akhir ini yang dapat digunakan sebagai masukan untuk pengembangan sistem enkripsi RSA dan penelitian lebih lanjut dari topik tugas akhir ini.