BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil pengujian pada waktu implementasi, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Teknik *kriptografi* yang digunakan untuk implementasi *HTTP* menggunakan *SSL* adalah teknik *kriptografi* asimetris. Teknik *kriptografi* ini mempunyai dua kunci yaitu kunci privat dan kunci publik. Kunci publik digunakan untuk mengenkripsi data yang akan dikirimkan oleh web browser dan untuk pendeskripsian disisi server menggunakan kunci private dari sertifikat server.
2. Pengesahan sertifikat digital dapat dilakukan sendiri oleh pemilik sertifikat dengan membuat *Certificate Authority* sendiri. Dari hasil pengujian, koneksi yang secure tetap bisa dibangun walaupun sertifikat tidak diakui oleh sebuah browser.
3. Ada dua pemodelan *web server* yang dapat diimplementasikan untuk *web server* yang menggunakan *SSL*, yaitu *web server* apache yang mendukung *HTTP* dan *HTTPS* diletakkan pada satu *web server*, dan yang kedua *web server* apache yang mendukung *HTTP* dan *HTTPS* diletakkan pada *web server* yang berbeda. Penggunaan dua model tersebut dapat diimplementasikan berdasarkan jenis kebutuhannya.

4. Dalam implementasi pengujian dengan menggunakan model *attacking sniffing* pada *gateway*, didapatkan kesimpulan pada saat pengaksesan aplikasi yang menggunakan protokol *HTTP*, *content* data yang dikirimkan melewati *gateway* tidak dienkripsi, sehingga informasi data berupa *username* dan *password* dapat disniffing. Sedangkan *content* data yang dikirimkan melewati *gateway* yang mengakses *URL HTTPS* akan dienkripsi, sehingga pada saat data tersebut disniffing, *content* data yang didapat dalam bentuk *ciphertext*.

5.2. Saran

Pengembangan ke depan supaya dimodifikasi dengan sistem *LDAP (Light Weight Directory Access Protocol)* sebuah protokol yang mengatur mekanisme pengaksesan *layanan direktori (Directory Service)*, supaya bisa menjadi satu kesatuan teknologi. *LDAP* sendiri mempunyai fungsi radius yang bisa dikembangkan dengan sistem *Hotspot* Sistem.