BAB VI
KESIMPULAN DAN SARAN

VI.1 KESIMPULAN

Kesimpulan yang dapat di ambil dari implementasi tugas akhir ini adalah :

1. Berdasarkan hasil monitoring menggunakan tools *wireshark* bahwa portal mahasiswa yang saat ini digunakan sistem autentikasinya tidak dienkripsi sehingga memungkinkan orang lain untuk mencuri username dan password.
2. Dengan penerapan algoritma kriptografi RSA dalam metode enkripsinya maka data tidak dapat dibaca oleh orang lain.
3. Penerapan SSL (*Secure Socket Layer*) menambah tingkat keamanan pada portal mahasiswa karena jalur komunikasi yang dilewati dienkripsi.
4. Aplikasi ini menambah tingkat keamanan di sisi *server* dengan pertama-tama mengenkripsi *plaintext password* menggunakan RSA sebelum kemudian di konvesi menjadi bentuk *hash* MD5. Teknik ini mencegah para *hacker* mendapatkan *plaintext* dari password dengan menggunakan teknik *brute force* atau melihat table *rainbow crack.*
5. Aplikasi ini dibangun dengan *JavaScript* pada sisi *client* dan PHP pada sisi *server.*

VI.2 SARAN

Beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut

1. Dapat dikembangkan untuk enkripsi di sisi *client* dengan membuat *plug-in* enkripsi RSA sehingga kunci publik tidak dapat dilihat oleh *client*.
2. Dapat dikembangkan di operating system lain seperti Ubuntu, FreeBSD, MacOS, dll.