BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan mengenai implementasi algoritma RC6 untuk keamanan *web login* dapat disimpulkan sebagai berikut :

1. Algoritma kriptografi RC6 dapat diimplementasikan pada *web login* untuk mengamankan data *username* dan *password* dengan baik.
2. Data *plaintext* atau *password* yang diinput oleh *user* dapat di enskripsi bersama kunci yang diberikan oleh sistem dengan algoritma RC6.
3. Dari pengujian yang dilakukan , sebanyak 30 query SQL Injection didapat 12 *query* berhasil menembus sistem *login* tanpa algoritma RC6. Tetapi setelah algoritma RC6 diimplementasikan pada sistem *login*, ke 30 *query* SQL *Injection* gagal menembus sistem.
4. Berdasarkan pengujian yang sudah dilakukan, algoritma RC6 terbukti mampu melindungi halaman *login* dari serangan SQL *Injection*.
5. Data *password* atau *plaintext* yang tersimpan di *database* sudah berbentuk *chipertext* , dimana akan susah dimengerti oleh manusia.

5.2 Saran

Berdasarkan hasil kesimpulan penelitian ini, peneliti memberikan beberapa saran diantaranya adalah sebagai berikut:

1. Akan lebih optimal jika panjang kunci ditambah ,semakin banyak kunci akan semakin komplex.

2. Aplikasi dapat dikombinasikan dengan algoritma kriptografi yang lain dengan mengikuti perkembangan ilmu keamanan data.
3. Karakter *plaintext* lebih diperbanyak atau ditambah lagi untuk proses enskripsi, sehingga akan semakin banyak *byte* yang digunakan.
4. Lebih baik lagi kalau aplikasi ini tidak hanya berjalan di *localhost* tapi juga bisa berjalan pada internet