BAB 5
PENUTUP

5.1 Kesimpulan

Kesimpulan yang dapat ditarik dari pembahasan dalam penelitian ini adalah sebagai berikut :

a. Implementasi kriptografi *one time pad* dalam mengamankan proses *login* pada sistem informasi akademik berjalan dengan baik sesuai yang diinginkan.
b. Dalam penelitian yang telah dilakukan *one time pad* dapat digunakan untuk penambahan keamanan *login* di sistem informasi akademik dengan menambahkan proses autentikasi *one time pad* sebelum *login* kedalam sistem informasi akademik.
c. Autentikasi *one time pad* dapat mencegah orang yang tidak berkepentingan untuk mencuri data-data yang bersifat pribadi sehingga sudah dirasakan cukup untuk meningkatkan pengamanan *login* sistem informasi akademik.
d. Keamanan pengenkripsian ini sangat bergantung pada kerahasiaan kunci rahasia yang digunakan baik dalam mengenkripsi maupun mendekripsi data atau informasi, karena walaupun untuk memecahkan sandi yang dibuat sangat sulit namun apabila kunci telah ditemukan akan sangat mudah untuk memecahkan sandi tersebut.
e. *Plaintext* harus berupa huruf agar proses enkripsi dapat berjalan karena apabila selain menggunakan huruf maka proses enkripsi tidak dapat berjalan/proses registrasi akun *one time pad* gagal dan panjang *plaintext* mempengaruhi panjang dari cipher
f. kriptografi *one time pad* memiliki kelemahan terhadap pencurian data dengan *sniffing* tetapi disini pencurian data *login* tersebut tidak bisa dicuri sepenuhnya karena ada *challange* untuk menginput 1 huruf dari *challange* yang sudah didaftarkan pada proses registrasi akun *one time pad*.

5.2 Saran

Dalam penelitian ini masih terdapat banyak kekurangan, oleh karena itu diperlukan saran untuk memperbaikinya. Berikut beberapa saran untuk penelitian berikutnya yang dapat dikemukakan :

a. Untuk menjamin kerahasiaan data dan informasi serta menjamin keamanan kunci rahasia yang digunakan maka kunci yang di*generate*harus benar-benar *random* atau acak dan hanya dapat dipergunakan sebanyak satu kali saja.
b. Kriptografi *one time pad* memiliki karakteristik besar *key* sama dengan besar *message*, maka sistem ini memiliki keterbatasan akan ukuran *message.*
c. Diharapkan dalam pengembangannya bisa menambahkan dengan metode pengamanan lainnya agar lebih aman dari pencurian data/*sniffing*.