BAB V
KESIMPULAN DAN SARAN

1.1 Kesimpulan

Kesimpulan yang dapat ditarik dari penelitian ini antaralain:

1. Penggunaan *hybryd cryptosystem* pada skema PEKS dimana algoritma kriptografi RC4 untuk mengenkripsi data dan algoritma kriptografi RSA untuk melindungi kunci RC4 membuat sistem dapat melindungi data sekaligus tidak menghamburkan media penyimpanan karena ukuran *file* yang dienkripsi oleh algoritma RC4 tidak akan berubah atau akan berukuran sama seperti *file* sebenarnya. Selain itu dengan memanfaatkan algoritma RSA, hanya pengguna yang terauthentifikasi yang dapat melakukan pencarian dan pengunduhan data. Hal ini sesuai dengan tujuan adanya kriptografi dalam hal kerahasian dan authentikasi.
2. Dengan memanfaatkan skema PEKS pada sistem yang dikembangkan tingkat keamanan data baik pada media penyimpanan maupun *database* mengalami peningkatan. Terbukti dari pemaparan pada bab empat sub-bab pengujian keamanan dengan menggunakan metode penyerangan pasif, penyerang tidak mendapatkan informasi yang berarti. Sama halnya seperti pada penyerangan pasif, dalam proses pencarian *server* juga tidak mendapatkan informasi yang berarti karena proses pencarian dilakukan dalam tabel data sementara yang hanya ada dalam satu kali proses pencarian. Ketika dicocokkan dengan *keywords* masukkan dari pengguna, data pada tabel data sementara diambil satu per satu untuk didekripsi kemudian baru dicocokkan. Dan berdasar pada sub-bab pengujian hasil pencarian, dari 5 percobaan dengan data yang berbeda skema PEKS terbukti dapat menemukan data terenkripsi.

1.2 Saran

Untuk penelitian selanjutnya diharapkan penelitan dapat meneliti poin-poin berikut :

1. Dalam proses pengunggahan modul, diharapkan *keywords* dari modul tersebut dapat diekstrak secara otomatis dari modul sehingga admin hanya perlu memilih *file* modul saja.
2. Dengan keterbatasan penelitian ini, diharapkan penelitian selanjutnya dapat melakukan pengujian pembobolan pesan yang telah terenkripsi.
3. Dalam pencarian data diharapkan dapat melakukan pencocokkan *keywords* dalam keadaan terenkripsi atau dalam bentuk cipherteks sehingga tingkat keamanan dapat lebih baik lagi.