BAB VII

PENUTUP

7.1 Kesimpulan

Berdasarkan studi serta analsis yang telah dilakukan baik terhadap teori maupun aplikasi yang dibuat, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. RSA adalah salah satu dari beberapa algoritma kriptografi asimetris yang menjadi standar defacto dunia untuk enkripsi asimetris.
2. Sebagai algoritma kriptografi asimetris, maka RSA juga mempunyai kunci yang berbeda untuk proses enkripsi dan dekripsi yang disebut kunci publik dan kunci privat.
3. Semua proses perhitungan pada algoritma RSA adalah operasional bilangan bulat.
4. Perhitungan pada enkripsi pada RSA samadengan perhitungan dekripsinya, hanya kuncinya saja yang berbeda.
5. Pada aplikasi yang dibangun, besar file hasil enkripsi kurang lebih adalah pajang digit kunci dikalikan besar file asal.
6. Untuk beberapa file waktu dekripsi lebih lama daripada waktu enkripsi, tapi ada beberapa jenis file yang sebaliknya.
7. Semakin panjang digit kunci yang digunakan untuk mengenkripsi, maka semakin susah untuk membongkar keamanan RSA

7.2 Saran

1. Untuk memperoleh tingkat keamanan yang baik gunakan bilangan prima yang panjang, maka dari itu program ini masih bisa dikembangkan lagi.
2. Dalam program ini pembengkakan file hasil enkripsi masih sangat besar, maka dari itu disarankan agar dalam membangun sebuah sistem kriptografi sebisa mungkin dapat dikombinasikan dengan program kompresi file.
3. Program ini sangat baik digunakan komunikasi data yang membutuhkan tingkat keamanan yang tinggi baik yang lingkupnya kecil (LAN) maupun yang lingkupnya lebih besar (internet). Seperti akses perbankkan melalui internet.