BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan uraian yang telah dijelaskan dalam skripsi mengenai algoritma kriptografi RSA,diperoleh kesimpulan sebagai berikut.

1. Konsep-konsep matematis yang melandasi pembentukan algoritma kriptografi RSA adalah divisible, algoritma pembagian, pembagi persekutuan terbesar, bilangan prima, persamaan kongruen, grup berhingga, pemetaan, dan Teorema Euler tentang persamaan kongruen.
2. Cara kerja algoritma kriptografi RSA terdiri dari proses pembangkitan kunci, proses enkripsi, dan proses dekripsi. Dan cara kerja aplikasi algoritma kriptografi RSA dalam tanda tangan digital terdiri dari proses pembangkitan kunci, proses sign digital signature, dan proses verifikasi digital signature.
3. Implementasi algoritma kriptografi RSA dalam program yang sederhana, yaitu program algoritma kriptografi RSA, dibuat menggunakan aplikasi Visual Basic 6.0.
4. Setelah dilakukan analisis dan perbandingan program kriptografi RSA menggunakan Visual Basic 6.0 yang dibuat penulis dengan program menggunakan IDE Microsoft Visual Studio 2010 yang dibuat Yudi Retanto dan Nikolaus Indra didapat hasil berupa kelebihan dan kekurangan pada program kriptografi RSA menggunakan Visual Basic 6.0 yang dibuat penulis. Kelebihan dari program kriptografi RSA menggunakan Visual Basic 6.0 yang dibuat penulis jika dibandingkan dengan program menggunakan IDE Microsoft Visual Studio 2010 adalah aspek waktu proses pembangkitan kunci dan enkripsi yang lebih cepat. Berikut hasil perbandingan waktu proses pembangkitan kunci dan enkripsi program kriptografi RSA

menggunakan Visual Basic 6.0 dengan program menggunakan IDE Microsoft Visual Studio 2010. Namun, program kriptografi RSA menggunakan aplikasi Visual Basic 6.0 yang dibuat penulis memiliki beberapa kekurangan. Karena program tersebut menggunakan tipe data `Double` yang terbatas pada $-1.79769313486232 \times 10^{308}$ sampai $-4.94065645841247 \times 10^{324}$ (Negatif) dan $1.79769313486232 \times 10^{308}$ sampai $4.94065645841247 \times 10^{324}$ (positif) sehingga perlu diperhatikan besarnya bilangan prima dan kunci publik yang akan dipilih. Lalu pada penghitungan nilai kunci pribadi perlu dihitung secara manual sehingga kurang praktis.

5.2 Saran

Berdasarkan uraian yang telah dijelaskan dan kesimpulan dalam skripsi mengenai algoritma kriptografi RSA, penulis memberikan beberapa saran sebagai berikut.

1. Algoritma kriptografi RSA dapat digunakan sebagai salah satu pilihan dalam menjaga dan mengamankan pesan rahasia karena sulitnya melakukan faktorisasi terhadap bilangan yang terbentuk dari dua bilangan prima yang besar sehingga tingkat keamanan algoritma kriptografi RSA cukup tinggi.
2. Perlu diperhatikan pemilihan bilangan prima dan dua kunci yang dibangkitkan dalam proses pembangkitan kunci untuk menjaga dari ancaman serangan-serangan terhadap keamanan algoritma kriptografi RSA.
3. Meski memiliki keterbatasan pada input bilangan, program kriptografi RSA dengan menggunakan aplikasi Visual Basic 6.0 yang dibuat penulis dapat digunakan sebagai alternatif dalam memahami algoritma kriptografi RSA.
4. Bagi penulis lain yang tertarik untuk membuat sebuah program sederhana mengenai implementasi dari algoritma kriptografi RSA, dapat menggunakan bahasa pemrograman lain serta aplikasi lainnya.