

BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan penjelasan dan pembahasan yang telah diuraikan pada bab – bab sebelumnya dan hingga tahap implementasi program. Maka dapat diambil kesimpulan bahwa :

1. Aplikasi ini dirancang sebagai media belajar kriptografi praktis dengan dilengkapi contoh perhitungan manual, penjelasan dan petunjuk penggunaan aplikasi dari masing – masing algoritma.
2. Setelah melakukan pengujian terhadap aplikasi dengan jumlah karakter pesan dan beberapa karakter (symbol, angka dan huruf) pada kriptografi RC4 dan DSA. Pada proses enkripsi dan dekripsi RC4 sudah sesuai dengan literature yang ada. Pada proses verifikasi pesan DSA, jika nilai $v = r$ sama maka tanda tangan sah dan pesan terverifikasi, dan jika nilai $v = r$ tidak sama maka tanda tangan tidak sah. Jika tidak sesuai dengan kunci sebenarnya maka hasil proses verifikasi tidak terverifikasi. Kunci *public*, kunci *private* merupakan angka jika kunci bukan angka maka aplikasi akan kembali ke tampilan sebelumnya. Dengan hasil tersebut maka aplikasi ini sudah berjalan dengan baik. Hasil proses enkripsi dan dekripsi kriptografi RC4 dan verifikasi pesan kriptografi DSA sesuai dengan perhitungan manual.

5.2 Saran

Dalam penulisan Skripsi ini tentu masih terdapat kekurangan, namun ini tidak menutup untuk disempurnakan untuk pengembangan selanjutnya agar dapat meningkatkan fungsional dan manfaat aplikasi ini. Beberapa saran untuk pengembangan aplikasi Kriptografi RC4 dan DSA ini yaitu :

1. Menambahkan algoritma kriptografi lain yang sesuai dengan *literature* yang ada sehingga ilmu dari aplikasi ini dapat lebih bermanfaat.
2. Pada proses pembentukan kunci kriptografi DSA dibuat pengecekan bilangan prima yang sesuai dengan *literature* kriptografi DSA yang menggunakan bilangan prima dalam proses pembentukan kunci, kunci *public*, dan kunci *private*.
3. Memperbaiki tampilan sehingga lebih menarik dan lebih *user friendly*.