BAB V

KESIMPULAN DAN SARAN

V.1. Kesimpulan

Dari uraian secara teoritis pada sistem perbandingan metode RSA dan MD5 dalam mengamankan pesan, maka penulis akan mencoba menarik kesimpulan dan akan memberikan saran-saran sebagai berikut:

1. Panjang pesan pada metode MD5 tidak boleh melebihi 264 bit sedangkan pada metode RSA boleh melebihi 264 bit tetapi tidak boleh melebihi 960 bit.
2. Nilai konstanta pada metode MD5 tidak unik hanya angka desimal sedangkan pada metode RSA nilai konstanta unik karena menggunakan bilangan HEX.
3. Dalam melakukan putaran metode MD5 sebanyak 4 kali sedangkan pada metode RSA melakukan putaran sebanyak 5 kali.
4. Hasil dari kalkulasi ke hash pada metode MD5 menghasilkan 128 *message bit* sedangkan metode RSA kalkulasi ke hash menghasilkan 160 *message bit*.
5. Perbandingan RSA dan MD5 menggunakan bahasa pemrograman visual basic 2010

V.1. Saran

Untuk menyempurnakan sistem yang telah dibuat, penulis memberikan saran-saran sebagai berikut:

1. Dalam mengamankan pesan ke hash dari kedua metode RSA dan MD5 lebih detail RSA dalam menangani *collution* terhadap serangan data karena proses

panjang pesan lebih panjang dari pada MD5 oleh karena itu lebih baik menggunakan RSA tetapi prosesnya kerja lebih lambat dari MD5.

2. Lebih baik menggunakan metode RSA karena nilai konstanta berupa HEX proses array lebih panjang bila dibandingkan MD5.
3. Jika dilihat dari perputaran RSA sebanyak 5 kali sedangkan MD5 sebanyak 4 kali oleh karena itu RSA lebih sedikit terjadinya *collusion*.
4. Dalam mengamankan pesan ke hash metode RSA lebih panjang daripada MD5 oleh karena itu lebih aman menggunakan RSA.