BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berikut kesimpulan dari Implementasi Algoritma BC3 dan RSA Dalam Sistem Keamanan Pesan *Electronic mail* (Email) adalah sebagai berikut:

1. Kombinasi dua algoritma kriptografi, algoritma BC3 dan algoritma RSA, dapat diimplementasikan untuk pengamanan pesan email. Pada proses enkripsi menghasilkan pesan rahasia atau *ciphertext* dalam format rangkaian blok biner 64 bit menggunakan algoritma BC3, dan kunci BC3 terenkripsi atau *cipherkey* dalam format rangkaian blok biner 128 bit menggunakan algoritma RSA. Pada proses dekripsi, *cipherkey* didekripsi terlebih dahulu menggunakan algoritma RSA untuk mendapatkan kunci BC3. Selanjutnya kunci BC3 tersebut akan mendekripsi *ciphertext* menjadi pesan sebenarnya menggunakan algoritma BC3. Berdasarkan analisis rasio jumlah bit plaintext dan ciphertext didapat nilai yang cukup signifikan yaitu berkisar 1:8. Hal tersebut terjadi karena format ciphertext berbentuk biner dan pada proses enkripsi terdapat proses padding yang akan mengakibatkan penambahan bit pada plaintext sehingga rasio bit ciphertext bernilai diatas dari 8.
2. Pengaruh kombinasi dua algoritma kriptografi, yaitu algoritma BC3 dan dan algoritma RSA, pada keamanan pesan email memenuhi 2 tujuan kriptografi yaitu kerahasiaan dan integritas data.
    a. Algoritma BC3 dapat menjaga kerahasiaan pesan pada proses pengiriman pesan. Proses enkripsi pada 50 data pesan menghasilkan 100% pesan acak (*ciphertext*) sehingga Proses dekripsi dilakukan dengan memodifikasi 1 bit pada *ciphertext* memperoleh 67.3% pesan masih acak. Sedangkan modifikasi 1 bit pada cipherkey pada proses dekripsi memperoleh 100% pesan masih acak. Dapat disimpulkan dari masing-masing pengujian

bahwa hasil yang diperoleh memiliki nilai diatas 50% sehingga memenuhi tujuan kriptografi yaitu kerahasiaan.

b. Aspek integritas data pada tujuan kriptografi terhadap implementasi algoritma BC3 dan RSA pada keamanan pesan terpenuhi. Hasil pengujian yang dilakukan menggunakan pasangan kunci yang berbeda pada proses dekripsi terhadap 50 data yaitu 100% *plaintext* yang tidak sesuai dengan *plaintext* asli. Sehingga penggunaan algoritma RSA dalam pertukaran kunci BC3 ini berpengaruh terhadap salah satu aspek tujuan kriptografi yaitu integritas data.

3. Berdasarkan lama waktu proses enkripsi diketahui rata-rata kecepatan proses enkripsi yaitu 8876.5138 bit/detik. Sedangkan untuk proses dekripsi memiliki rata-rata kecepatan proses dekripsi 13775.3 bit/detik. Berdasarkan kecepatan masing-masing proses, dapat disimpulkan bahwa penambahan algoritma RSA dan konversi biner ke desimal tidak terlalu menambah waktu pada proses dekripsi. Terlihat dari rata-rata kecepatan proses enkripsi lebih lambat daripada proses dekripsi. Hal tersebut terjadi karena pada proses enkripsi terdapat proses padding.

5.2. Saran

Berikut merupakan saran terhadap penelitian ini untuk pengembangan lebih lanjut:

1. Perlu diadakannya pengembangan lebih lanjut terkait sistem yang dibuat berupa *attachment file*, seperti berkas dokumen, gambar, animasi, video, dan lainnya. Pengembangan juga dapat dilakukan dengan menggunakan berbagai macam *mail server*, sehingga kompatibel terhadap *mail server lain*.
2. Menggunakan bahasa pemrograman selain Matlab seperti PHP, Java atau bahasa pemgrograman lannya yang lebih kompatibel pada tampilan antarmuka pengiriman dan penerimaan email.
3. Penggunaan algoritma RSA digunakan tidak hanya untuk pertukaran kunci namun sebagai *digital signature*.

4. Penambahan keamanan pada pengiriman kunci menggunakan algoritma kriptografi lain, seperti ECDSH dan sebagainya.