BAB V

SIMPULAN DAN SARAN

5. 1. Simpulan

Kesimpulan yang didapat dari hasil penelitian yang telah dipaparkan sebelumnya antara lain sebagai berikut:

1. Kombinasi algoritma *Diffie-Hellman* dan RSA terletak pada proses pembangkitan kunci, di mana mulanya dilakukan pembangkitan kunci dengan algoritma *Diffie-Hellman* kemudian dilanjutkan dengan algoritma RSA sehingga menghasilkan kunci publik dan kunci privat. Adapun pada proses enkripsi *file excel* dan dekripsi *file excel* menerapkan perhitungan algoritma RSA dengan kunci yang sebelumnya telah didapat pada proses pembangkitan kunci.
2. Program aplikasi implementasi *Diffie-Hellman-RSA* dalam pengamanan data pada *file excel* memiliki tiga program utama, yaitu pembangkitan kunci, enkripsi dan dekripsi. Program pembangkitan kunci menghasilkan kunci publik untuk proses enkripsi *file* dan kunci privat untuk proses dekripsi *file.* Program enkripsi menghasilkan suatu *file excel* yang telah dienkripsi dengan kunci publik sehingga isi dari *file excel* tidak dapat terbaca. Sedangkan program dekripsi mengembalikan isi dari *file excel* seperti semula sebelum proses enkripsi.

5. 2. Saran

Adapun saran untuk penelitian selanjutnya adalah:

1. Mengkaji kembali penggunaan algoritma *Diffie-Hellman-RSA* dengan tujuan mencari cara agar hasil enkripsi tidak memberikan nilai cipherteks yang berpola.
2. Mengkaji algoritma kriptografi lain serta membandingkan dengan algoritma *Diffie-Hellman-RSA* untuk menemukan algoritma terbaik dalam pengamanan data pada *file excel* baik dari segi keamanan, maupun waktu yang dibutuhkan dalam proses enkripsi dan dekripsi data.

3. Menghadirkan suatu sistem keamanan untuk otentikasi pengirim pesan dan penerima pesan sehingga mencegah resiko manipulasi kunci publik oleh *man-in-the-middle*.
4. Memperluas cakupan masalah, seperti mengkonstruksi program aplikasi komputer untuk pengamanan data pada *file excel* yang juga dapat mengenkripsi dan mendekripsi gambar, simbol, ataupun formula *excel* di dalam *file* tersebut.