BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melalui tahap perancangan sistem dan implementasi, serta berdasarkan uraian dan pembahasan pada bab-bab sebelumnya maka dapat diambil beberapa kesimpulan, yaitu:

1. Perangkat lunak aplikasi yang dibangun dapat menangani proses enkripsi, dekripsi, tanda tangan digital dan verifikasi dengan baik, sehingga mampu memberikan keamanan yaitu aspek kerahasiaan dan autentikasi data.
2. Pada semua proses yang ditangani algoritma RSA dan El Gamal, ukuran kunci berbanding lurus dengan waktu/kecepatan proses.
3. Pada proses enkripsi, El Gamal mampu menyelesaikan proses lebih cepat dibanding RSA. Sedangkan pada proses pembangkitan kunci, RSA lebih unggul dibanding El Gamal.
4. Ukuran cipher yang dihasilkan algoritma kunci publik RSA dan El Gamal lebih besar dibandingkan dengan ukuran file asli sebelum enkripsi. Dan RSA terbukti lebih efisien dalam proses enkripsi karena menghasilkan cipher berukuran lebih kecil dari cipher El Gamal yang bahkan ukurannya 2 kali lipat lebih besar daripada cipher RSA.

5.2 Saran

Berbagai macam perangkat lunak aplikasi tidak menutup kemungkinan untuk terus dikembangkan dan disempurnakan, begitu pula dengan aplikasi ini. Berikut adalah beberapa saran yang dipandang perlu dalam proses pengembangan berikutnya:

1. Disarankan untuk menerapkan metode pemampatan data pada file cipher untuk menekan pembengkakan ukuran file cipher yang besar.
2. Perlu diadakan penelitian yang lebih mendalam tentang tingkat keamanan sistem kriptografi kunci publik khususnya pada algoritma RSA dan El Gamal.