BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan penjelasan yang terdapat pada bab awal sampai akhir dari "Analisis dan Perancangan Kriptografi Hybrid dengan Algoritma RSA, AES128, dan SHA-1 untuk Pengiriman File Document ", maka dapat disimpulkan :

1. Proses perancangan aplikasi yang dibuat ini telah sesuai dengan latar belakang masalah dan batasan masalah yang ada.
2. Pengimplementasian algoritma Hybrid RSA, AES128, SHA-1 untuk mengamankan informasi pesan email telah berhasil dibuat. Aplikasi yang dibangun tersebut dapat melakukan proses pembangkitan kunci dan penyimpanan kunci kedalam file teks *.txt* atau *.doc*. Pengenkripsian pesan teks maupun *document* serta mengirim pesan yang telah dienkripsi berjalan dengan baik.
3. Symmetric Key Standar AES menggunakan kunci rahasia yang sama dibagi antara pengirim dan penerima, yang akan digunakan untuk enkripsi maupun dekripsi.
4. Asimetris standar key RSA menggunakan sepasang kunci dari *public key* dan *private key*. Umumnya, *public key* digunakan untuk enkripsi pada pengirim akhir dan sebuah *private key* digunakan untuk dekripsi pada akhir penerima. Juga keaslian data dan integritas didirikan dengan menggunakan tanda tangan digital.

5. Algoritma Hybrid (RSA, AES128, dan SHA-1) dikarenakan algoritma asimetris sangat matematika intensif mereka tidak besar pada enkripsi volume data yang besar, sehingga Anda dapat membuat kunci sesi sementara yang Anda mengenkripsi dengan RSA dan kemudian menggunakannya kunci sesi untuk mengenkripsi data anda yang lebih besar dengan algoritma simetris seperti AES.

5.2 Saran

Dalam penulisan skripsi ini tentunya masih terdapat banyak kekurangan, namun tidak menutup kemungkinan untuk dapat disempurnakan untuk pengembangan selanjtnya serta dapat meningkatkan fungsional dan manfaat dari aplikasi ini. Beberapa hal yang mungkin dapat dilakukan untuk pengembangan aplikasi ini yaitu :

1. Memperbaiki *Graphical User Interface* (GUI) agar lebih menarik dan lebih *user friendly*.
2. Menambahkan fitur Terima Pesan dalam aplikasi.
3. Menambahkan fitur Dekripsi pesan dan file terpisah.
4. Menambahkan fitur terima file agar saat mengambil file, sehingga tidak melalui gmail.