BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan uraian yang telah dijelaskan pada penelitian ini, maka diperoleh kesimpulan sebagai berikut:

a. Penyandian pesan dengan menggunakan kriptografi *hybrid autokey* Vigènere *cipher* dan algoritma El Gamal adalah sebagai berikut:
   1. Penyandian pesan dengan menggunakan kriptografi *hybrid autokey* Vigènere *cipher* dan algoritma El Gamal terbagi menjadi tiga tahap utama, yaitu pembangkitan kunci El Gamal, enkripsi dan dekripsi.
   2. Pembangkitan kunci El Gamal dan dekripsi dilakukan oleh penerima pesan. Sedangkan, enkripsi dilakukan oleh pengirim pesan.
   3. Proses enkripsi dan dekripsi *autokey* Vigènere *cipher* tidak hanya diperuntukkan untuk *alphabet* saja, melainkan diperluas berdasarkan 256 kode ASCII.
   4. Pada kunci publik dan privat yang sama, memungkinkan diperoleh cipherteks yang berbeda-beda dikarenakan pembangkitan k secara acak.
   5. Cipherteks yang dihasilkan dua kali lipat dari plainteksnya.
b. Program aplikasi dapat digunakan untuk menyandikan pesan dan megembalikan pesan sandi.

5.2 Saran

Saran dari penulis adalah sebagai berikut:

a. Diteliti perbandingan performa antara kriptografi *hybrid* metode dua tingkatan kunci (yang penulis pakai) dan kriptografi *hybrid* metode pertukaran kunci, di mana algoritma asimetris digunakan untuk mengenkripsi dan mendekripsi kunci simetris.
b. Diteliti lebih lanjut keamanan dari kriptografi *hybrid autokey* Vigènere *cipher* dan algoritma El Gamal.