BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan pada bab sebelumnya, maka diperoleh kesimpulan sebagai berikut:

1. Penyamaran pesan teks dengan kriptografi *hybrid atbash-autokey cipher* dan algoritma El Gamal, dilakukan dengan mengikuti rancangan skema *hybrid* dengan tiga tahapan utama yaitu pembangkitan kunci, enkripsi dan dekripsi. Tahapan 'Pembangkitan Kunci' dilakukan untuk mendapatkan kunci publik dari algoritma El Gamal. Pada tahap 'Enkripsi', pesan asli akan disamarkan dengan *atbash cipher*, dilanjutkan dengan *autokey cipher* (menggunakan kunci *autokey*), kemudian dengan algoritma El Gamal (menggunakan kunci publik) hingga menghasilkan pesan tersamar. Pada tahap 'Dekripsi', pesan tersamar akan dikembalikan dengan algoritma El Gamal (menggunakan kunci privat), dilanjutkan dengan *autokey cipher* (menggunakan kunci *autokey*), kemudian dengan *atbash cipher* hingga menghasilkan pesan asli.
2. Program aplikasi dibuat dengan bahasa *Graphical User Interf*ace (GUI) Python, menghasilkan program aplikasi yang *user-friendly*. Terdapat empat menu utama, yaitu *key generator*, *encrypt*, *decrypt*, dan uji *avalanche effect*. Menu *key generator* dan *decrypt* digunakan oleh penerima pesan untuk mengembalikan pesan tersamar dan menu *encrypt* digunakan oleh pengirim pesan untuk menyamarkan pesan. Sementara menu uji *avalanche effect* digunakan untuk mengukur tingkat keamanan kriptografi.
3. Berdasarkan pengujian yang telah dilakukan, terlihat bahwa walaupun kriptografi *atbash* dan *autokey cipher* dapat menyamarkan pesan, tetapi algoritma El Gamal dapat mengamankan jauh lebih baik. Kriptografi hybrid yang diusulkan dapat meningkatkan tingkat keamanan dibandingkan kriptografi tunggal, tetapi tidak signifikan dalam menjaga keamanan pada pesan teks (dikarenakan *k* acak).

5.2 Saran

Berikut adalah saran yang dapat diterapkan untuk penelitian selanjutnya.

1. Untuk penelitian selanjutnya diharapkan melakukan pengujian terhadap implementasi kriptografi yang telah dilakukan, baik dengan pengujian *avalanche effect* (AE) maupun pengujian lainnya.
2. Penelitian ini hanya menggunakan pengujian *avalanche effect* (AE), sehingga disarankan untuk melakukan perbandingan terhadap kriptografi *hybrid* dengan pengujian lainnya, yaitu *strict avalanche criterion* (SAC), *Completeness*, dan lainnya.
3. Untuk penelitian selanjutnya diharapkan melakukan perbandingan *running time* antara kriptografi tunggal dan kriptografi *hybrid*.