BAB V
KESIMPULAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan yang telah dipaparkan pada bab-bab sebelumnya, maka ditarik kesimpulan sebagai berikut:

1. Pengamanan Pesan Teks dengan Kriptografi *Lightweight Present Cipher* pada *Cipher Block Chaining* dilakukan dengan menkonversi plainteks dan kunci input menjadi bitstring. Setelah itu, plainbit dibagi menjadi beberapa plainblok. Berikutnya, plainblok dienkripsi dengan kuncibit yang sudah di-*padding* atau di-*cutting*. Hasil enkripsi setiap plainblok disebut dengan cipherblok yang berikutnya digabung untuk menghasilkan cipherbit. Setelah itu, cipherbit dikonversi menjadi cipherteks. Proses dekripsi dapat diperoleh dengan membalikkan proses enkripsi. Serangkaian proses tersebut diilustrasikan oleh sebuah skema sehingga dapat memberikan gambaran yang lebih jelas untuk membuat *pseudocode* algoritma yang diterapkan pada Aplikasi *Lightweight Present*.
2. *Pseudocode* algoritma yang telah dibuat diterapkan pada Aplikasi *Lightweight Present* dengan Bahasa pemrograman Python. Begitu juga dengan UI (*User Interface*) dari Aplikasi *Lightweight Present* dibuat dengan Bahasa pemrograman Python. UI dibuat sedemikian sehingga pengguna dapat mengamankan pesan teks menggunakan Aplikasi *Lightweight Present*.
3. Validasi dilakukan mengikuti skema Aplikasi Lightweight *Present* Cipher dengan bantuan Excel. Terdapat 6 tahap validasi. Hasil validasi menunjukkan bahwa hasil yang dikeluarkan program sama dengan hasil yang dikeluarkan Excel di setiap tahapnya. Oleh karena itu, program Aplikasi Lightweight *Present* Cipher dapat dikatakan telah divalidasi.

5.2 Saran

Setelah melakukan penelitian mengenai Pengamanan Pesan Teks dengan Kriptografi *Lightweight Present Cipher*, adapun saran dari penulis untuk penelitian selanjutnya adalah

1. Mengembangkan pengamanan pesan dengan kriptografi *Lightweight Present Cipher* untuk pesan berupa gambar, audio, atau vidio.
2. Mengembangkan pengamanan pesan dengan kriptografi *Lightweight Present Cipher* menggunakan mode operasi *Block Cipher* yang berbeda misalnya *Cipher Feedback (CFB), Output Feedback (OFB),* atau *Counter (CTR).*