BAB V
KESIMPULAN, IMPLIKASI DAN REKOMENDASI

Pada bab ini akan dirangkum beberapa hal berdasarkan temuan dan bahasan pada bab sebelumnya.

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan pada bab sebelumnya, berikut ini kesimpulan yang dapat diambil dari penelitian ini:

1. Untuk meningkatkan keamanan pengenkripsian Caesar *Cipher* menggunakan enkripsi *Row Transposition Cipher* dilakukan enkripsi bertahap. Enkripsi Caesar *Cipher* dilakukan terlebih dahulu dengan rumus enkripsi C = P + b (mod 26) , dimana C adalah orde dari karakter *ciphertext*, P orde dari karakter *plaintext* dan b adalah banyaknya kunci atau pergeseran yang dipilih. Kemudian *ciphertext* hasil enkripsi Caesar *Cipher* dienkripsi kembali menggunakan enkripsi *Row Transposition Cipher* dengan rumus enkripsi C= $\bigcup_{=1}$ K_i dengan n adalah banyaknya kolom yang dibuat dalam pengenkripsian, K_i adalah kolom-kolom ke *i* , *i* adalah urutan dari kunci pengenkripsiannya (dengan tanpa mengurangi keumuman). Kunci yang mungkin dari hasil enkripsi bertahap tersebut adalah 26 x n x n!. Sehingga, apabila n yang dipilih sangat besar, maka kunci yang mungkin dari pengenkripsiannya juga sangat besar, akibatnya seorang *cryptanalyst* harus menggunakan teknik *brute force search* untuk mendapatkan kunci enkripsi Caesar *Cipher* yang telah ditingkatkan keamanannya ini.

2. Untuk mengkontruksi suatu program aplikasi, dirancang terlebih dahulu hal-hal dasar dalam pembuatan aplikasi, yaitu, menentukan skema dari program aplikasi. Setelah itu, dibuat algoritma program berdasarkan skema yang telah dibuat, lalu, dikembangkan kode program dari program aplikasi. Setelah program aplikasi berjalan dengan baik, kemudian tampilan program aplikasi diatur sehingga terlihat rapih.

5.2 Implikasi

Saat ini tingkat pencurian data di internet sangat tinggi, oleh karena itu pengguna internet harus berhati-hati dalam memasukan informasi yang bersifat pribadi atau rahasia di internet. Aplikasi pengirim *email* yang telah dibuat pada penelitian ini dapat digunakan untuk memastikan bahwa pesan *email* yang dikirim tetap aman, sebab pesan yang dikirim merupakan pesan terenkripsi yang hanya dapat dibaca oleh pemilik kunci enkripsinya.

5.3 Rekomendasi

Setelah melakukan peningkatan keamanan enkripsi Caesar *Cipher* dan mengaplikasikannya pada program aplikasi pengirim *email*, diharapkan peneliti selanjutnya dapat mengembangkan aplikasi pengirim *email* yang telah dibuat dengan jumlah karakter yang lebih banyak lagi dan penggunanya tidak terbatas pada pemilik akunYahoo Mail dan Google Mail.