BAB V

PENUTUP

5.1 Kesimpulan

Dari uraian yang telah disampaikan pada bab-bab sebelumnya tentang implementasi metode *Cipher Classic* ini, dapat diambil kesimpulan sebagai berikut.

1. Metode *Cipher Classic* ini hanya menggunakan 26 huruf alphabet, sehingga hasil enkripsinya pun juga berupa huruf.
2. Pada metode *Columnar Transposition* walaupun digunakan kata kunci yang berbeda namun hasil enkripsinya bisa sama.
3. Pada metode *Caesar Cipher* dan *Vigenere Cipher*, terdapat satu kesamaan yaitu apabila *plaintext* yang dimasukkan sama dan kedua metode tersebut dienkripsi dengan kata kunci menggunakan huruf ‘A’ tanpa penambahan huruf lain (untuk metode *Vigenere Cipher*), maka hasil enkripsinya akan sama dengan *plaintext* yang dimasukkan.
4. Dari ketiga metode tersebut, metode *Vigenere Cipher* merupakan metode yang paling baik untuk digunakan dalam mengenkripsi text. Dalam metode ini digunakan perhitungan yang cukup rumit dalam mengenkripsi text dibandingkan dengan metode yang lain, yaitu dengan merubah huruf *plaintext* dan kata kunci dalam bentuk angka dan menjumlahkan angka tersebut lalu membaginya dengan modulo 26. Hasil angka yang didapat akan dirubah ke huruf kembali. Walaupun digunakan kata kunci yang berulang sesuai panjang plaintext tetapi hasil enkripsinya akan sulit untuk ditebak karena frekuensi huruf menjadi tidak jelas. Metode ini merupakan

Polyalpabetic substitution chiper yang kebanyakan program keamanan komputer (*computer security*) menggunakan *chiper* jenis ini.

5.2 Saran

Pada implementasi metode *Cipher Classic* ini masih jauh dari sempurna, masih banyak hal yang perlu diteliti dan di analisis. Melalui implementasi ini diharapkan agar pengguna mampu mengembangkan program bantu untuk menganalisa metode *Cipher Classic* ini menjadi sebuah aplikasi yang lebih kompleks lagi, sehingga dampak yang dihasilkan menjadi lebih bisa dirasakan oleh penggunanya. Pada sistem ini masih terdapat kekurangan yang dapat diperbaiki dimasa yang akan datang antara lain yaitu:

1. Dalam sistem ini masih dapat dikembangkan ke dalam bentuk jaringan, yaitu berupa pengiriman *e – mail* dengan pesan yang dienkripsi menggunakan algoritma *Cipher Classic* dengan ketiga metode tersebut (*Caesar Cipher, Columnar Transposition* dan *Vigenere Cipher*).
2. Dalam analisis pada implementasi program ini belum dibahas tentang bagaimana cara pemecahan masing – masing metode dan pemecahan pesan yang telah terenkrip tanpa diketahui kata kuncinya. Untuk itu, pengembang diharapkan lebih bisa menganalisa algoritma *cipher classic* ini yang dikhususkan pada pemecahan kata kuci yang digunakan untuk mengenkrip dan mendekrip pesan serta memecahkan pesan yang telah dienkripsi.
3. Dalam program implementasi algoritma *Cipher Classic* ini (*Caesar Cipher, Columnar Transposition* dan *Vigenere Cipher*) belum di tambah dengan adanya proses penyimpanan text yang telah dienkripsi. Untuk itu diharapkan para pengembang dan juga para pengguna program ini mampu

mengembangkannya sehingga menjadikan program ini lebih bisa dirasakan oleh penggunanya.