

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan rumusan masalah dan tujuan penelitian serta isi yang telah diuraikan, maka dapat disimpulkan beberapa hal antara lain:

1. Kriptografi dengan cara *caesar cipher* dan *affine cipher* yaitu dengan menukar setiap huruf asli dengan huruf yang lain. Penukaran ini menggunakan cara *shift transformation* untuk *caesar cipher* dan *affine transformasion* untuk *affine cipher*. Pengkomposisian kriptografi *caesar cipher* dan *affine cipher* dengan cara dua kali enkripsi dan dua kali dekripsi secara berurutan.
2. Konsep – konsep matematika yang digunakan dalam kriptografi komposisi *caesar cipher* dan *affine cipher* yaitu fungsi komposisi, GCD, relatif prima, modulo, algoritma eulcid. Lebih lanjut lagi diperoleh suatu hubungan bahwa kriptografi enkripsi *caesar cipher* dan *affine cipher* merupakan fungsi bijektif (satu-satu dan pada), dan himpunan bilangan bulat dengan operasi rumus enkripsi *caesar cipher* adalah grup.
3. Perancangan program kriptografi komposisi *caesar cipher* dan *affine cipher* diawali dengan membuat *flowchart* enkripsi dan dekripsi, kemudian membuat desain tampilan program. Pembuatan program aplikasi kriptografi menggunakan bahasa pemrograman Delphi 7. Pengujian program dilakukan dengan cara membandingkan hasil manual dengan hasil pada program. Berdasarkan hasil perbandingan tersebut, hasil yang diperoleh dari keduanya sama. Hal ini menunjukkan bahwa program telah sesuai dengan yang diinginkan.

5.2 Saran

Berikut saran yang ditujukan untuk pengembangan program aplikasi komposisi kriptografi adalah mencari metode lain selain komposisi dalam memperkuat kriptografi, kemudian dapat mengembangkan karakter yang tidak terbatas hanya pada 95 karakter.