BAB V
KESIMPULAN DAN REKOMENDASI

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat disimpulkan bahwa:

1. Konsep algoritma *Hill cipher* yang dimodifikasi menggunakan *convert between base* adalah mengkonversi plainteks yang sudah dikonversi ke dalam kode ASCII dalam suatu basis tertentu ke basis lainnya menggunakan *convert between base*.
2. *Linear feedback shift register* biasa digunakan untuk pembangkit *Stream cipher* yang berbasis biner sedangkan Hill cipher berbasis alfabet. Dengan menggunakan *convert between base* maka *linear feedback shift register* dapat diterapkan pada *Hill cipher* dengan cara pembangkitan kunci, proses convert between base, peng-XOR-an kemudian diterapkan pada *Hill cipher*.
3. Implementasi algoritma modifikasi *Hill cipher* dalam bentuk program aplikasi dapat dibuat dengan menggunakan MATLAB. MATLAB mendukung aljabar linear khususnya mengenai matriks sehingga modifikasi Hill cipher dapat diimplementasikan.
4. Modifikasi *Hill cipher* dapat digunakan untuk enkripsi dan dekripsi. Modifikasi ini juga sudah memenuhi sistem kriptografi. Penggunaan *convert between base* dan pembangkitan kunci dengan *linear feedback shift register* dapat memperkuat keamanan algoritma kriptografi. Hal ini ditunjukkan dengan tidak terpecahkannya kunci pada saat dilakukan kriptanalisis. Selain itu ditunjukkan pula ketersediaan kunci dan banyaknya kemungkinan yang dimiliki oleh kunci *linear feedback shift register* dan matriks kunci untuk dipecahkan sehingga akan mempersulit kriptanalis dalam memecahkan kunci dan menemukan plainteks.

5.2 Rekomendasi

Untuk pengembangan lebih lanjut, maka penulis memberikan rekomendasi yaitu analisa mengenai kebutuhan memori karena keamanan algoritma dapat

diekuivalenkan juga dengan memori. Selain itu juga dapat digunakan kode extended-ASCII sehingga lebih banyak karakter yaitu sebanyak 255 karakter.