BAB V

PENUTUP

5.1 Kesimpulan

Dari analisis perancangan dan implementasi yang telah dilakukan, telah berhasil dibuat Aplikasi enkripsi pesan singkat berbasis Android menggunakan kombinasi Algoritma Vigenere Cipher dan *Advanced Encryption Standard* (AES) 128. Berikut kesimpulan dari penelitian tersebut :

1. Aplikasi dapat mengirimkan pesan terenkripsi dan dapat melakukan dekripsi kembali apabila kunci yang dimasukkan sudah sesuai.
2. Perubahan *plaintext* menjadi *ciphertext* pada algoritma Vigenere Cipher dilakukan dengan mengubah karakter menjadi bilangan desimal yang disesuaikan dengan table ASCII, setelah itu dilakukan penjumlahan dan mod untuk mendapatkan hasil enkripsi menggunakan algoritma Vigenere Cipher.
3. Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dimasukkan ke dalam *state* akan mengalami transformasi byte AddRoundKey. Setelah itu, *state* akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, *state* tidak mengalami transformasi MixColumns.

4. Aplikasi dapat berjalan dengan baik pada beberapa *device* Android dengan karakteristik yang berbeda-beda, namun terdapat kendala dalam proses deskripsi pada Android yang memiliki OS 4.2.

5.2 Saran

Beberapa saran untuk pengembangan aplikasi ini selanjutnya yaitu:

1. Pengembangan selanjutnya pada aplikasi ini menggunakan algoritma Asimetri, sehingga kunci akan sulit dipecahkan oleh kriptanalisis karena kunci yang digunakan untuk enkripsi dan dekripsi berbeda.
2. Diharapkan dilakukan pengembangan lebih lanjut pada *platform mobile* lainya, seperti iOS, Blackberry OS dan Windows *Phone*.