BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari penelitian Implementasi Kriptografi AES dan OTP dalam Membangkitkan Kode Otentikasi untuk Aktivasi *Online Member* Baru yang dikirim melalui SMS adalah sebagai berikut.

1. Kode otentikasi berbasis heksadesimal dapat dibangkitkan dengan mengenkripsi pesan aktivasi yang ditambah dengan timestamp menggunakan algoritma kriptografi *Advance Encryption Standard* 256 *bits* yang telah dimodifikasi pada tahapan membangkitkan S-Box dan fungsi *ShiftRow* dengan menjadikan password akun sebagai *private key*. Untuk timestamp sendiri akan dipakai untuk memberikan masa penggunaan kode pada metode *One Time Password*. Sehingga kode otentikasi yang dibangkitkan memiliki masa penggunaan dan hanya bisa digunakan satu kali.
2. Setelah pendaftar mendaftarkan akun baru miliknya dan menerima SMS kode otentikasi yang dikirimkan sistem, maka pengguna dapat mengaktivasi akun miliknya dengan memasukan username, password dan kode otentikasi yang diterima, selanjutnya sistem akan mencari ciphertext pasangan dari kode otentikasi, setelah ciphertext pasangan dari kode otentikasi ditemukan maka ciphertext akan didekripsi dengan algoritma kriptografi *Advance Encryption Standard* 256*bits* yang telah dimodifikasi menggunakan kunci berupa *password* milik pendaftar, hasil dari dekripsi ciphertext tersebut berupa pesan aktivasi dan timestamp, setelah pesan aktivasi divalidasi dan sisa waktu masa penggunaan kode otentikasi telah divalidasi maka akun dari pendaftar berhasil diaktifkan.

3. *Advance Encryption Standard* yang telah dimodifikasi berhasil diuji dengan menggunakan pengujian nilai *Avalanche Effect* dan pengujian *Randomness Test,* dimana untuk pengujian nilai *Avalanche Effect* algoritma yang baik akan menghasilkan nilai sekitar 50% dengan beberapa kondisi tes, dan untuk pengujian *Randomness Test* hasil enkripsi berupa ciphertext berhasil lolos melaui beberapa opsi tes yang diberikan seperti *Frequency test, Poker Test, Run Test, Long Run Test,* dan *Serial Test.*

5.2 Saran

Berikut merupakan saran-saran pada penelitian ini untuk pengembangan lebih lanjut:

1. Perlu ditingkatkan kembali kompleksitas untuk Algoritma kriptografi *Advance Encryption Standard* dengan cara melakukan *Hash-ing* pada kunci.
2. Modifikasi dapat dilakukan dengan menggunakan dua prinsip Shannon yaitu *Confusion* dan *Diffusion* pada bagian lainnya seperti *MixColumns, SubByte,* atau *AddRoundKey* untuk meningkatkan nilai kompleksitasnya.