BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari penelitian implementasi Algoritma RC6 dan metode *One Time Password* pada proses pembuatan kode otentikasi untuk *website online marketplace* adalah sebagai berikut.

1. Penerapan algoritma RC6 untuk mengenkripsi dan mendekripsi waktu pembangkitan kode aktviasi berhasil diimplementasikan pada proses pembuatan kode otentikasi untuk *website online marketplace*. Kemudian, penerapan metode HOTP untuk membangkitkan kode aktivasi dengan menggunakan *ciphertext* dari hasil proses enkripsi sebagai kunci rahasia dan *counter* dari pembangkitan kode aktivasi berhasil diimplementasikan pada proses pembuatan kode otentikasi untuk *website online marketplace*.
2. Hasil pengujian Avalanche Effect terhadap ciphertext yang dihasilkan oleh algoritma RC6 menunjukan hasil yang sangat baik yakni 50,20%. Hasil dari pengujian Statistical Randomness Test mulai dari pembangkitan kunci enkripsi dengan LCG, proses enkripsi dengan algoritma RC6 serta pembangkitan kode aktivasi dengan menggunanakan HOTP menunjukan hasil yang sangat bagus yakni dengan dinyatakannya lolos uji keacakan dengan hasil yakni dari nilai rata-rata pengujian frequency sebesar 0,966666667 yang tidak melebihi nilai maksimum dari pengujian frequency yakni 6,635, nilai rata-rata pengujian poker sebesar 9,25 yang tidak melebihi nilai maksimum dari pengujian poker yakni 30,58, nilai rata-rata pengujian run sebesar 5,549248233 yang tidak melebihi nilai maksimum dari pengujian run yakni 13,28, nilai rata-rata pengujian long run sebesar 7,230403967 yang tidak melebihi nilai maksimum dari pengujian long run yakni 34 dan nilai rata-rata pengujian serial sebesar 2,784898467 yang tidak melebihi nilai maksimum dari pengujian serial yakni 9,21. Kedua pengujian tersebut menunjukan bahwa penerapan Algoritma RC6 dan metode *One Time Password* pada proses pembuatan kode otentikasi untuk

Yogi Siswanto, 2019
IMPLEMENTASI LCG, ALGORITMA RC6 DAN OTP UNTUK MEMBANGKITKAN KODE OTENTIKASI WEBSITE ONLINE MARKETPLACE MELALUI SMS
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

website online marketplace memenuhi unsur-unsur kriptografi yakni kerahasiaan dan integritas data.

3. Hasil pengujian keamanan dengan menggunakan serangan *Man In The Middle* yang menunjukan hasil bahwa sistem yang telah dibuat tahan terhadap serangan yang dilakukan dengan cara mencuri kode aktivasi atau mengganti kode aktivasi asli dengan kode aktivasi palsu pada jalur pengiriman kode aktivasi pada saat server mengirimkan kode aktivasi kepada pengguna dengan atau tanpa mengetahui username dan password dan juga pada jalur pengiriman kode aktivasi pada saat pengguna mengirimkan kode aktivasi kepada server dengan atau tanpa mengetahui username dan password. Kemudian, hasil pengujian keamanan dengan menggunakan *password guessing attack* yang menunjukan bahwa sistem yang telah dibuat memiliki peluang keberhasilan yang sangat kecil yakni sebesar 1×10^{-6}. Nilai tersebut menunjukan bahwa, 1 dari 3 kali kesempatan proses pencocokan kode aktivasi sama dengan salah satu kode OTP yang sebelumnya dibangkitkan sebanyak 10^6. Selain itu, dengan memberikan batasan jumlah pencocokan dalam proses aktivasi dapat memperkecil kemungkinan berhasilnya password guessing attack. Hasil tersebut lebih kecil dibandingan dengan peluang keberhasilan dari serangan exhaustive yakni sebesar $\frac{10^6}{10^6}$ dengan tanpa batasan jumlah proses aktivasi. Kedua pengujian tersebut menunjukan bahwa penerapan Algoritma RC6 dan metode *One Time Password* pada proses pembuatan kode otentikasi untuk *website online marketplace* memenuhi unsur-unsur kriptografi yakni otentikasi dan nir-penyangkalan.

5.2 Saran

Berikut ini merupakan saran untuk pengembangan penelitian selanjutnya.

1. Penelitian selanjutnya dapat memodifikasi algoritma RC6 agar hasil dari pengujian *Avalanche Effect* bisa mendapatkan hasil yang lebih mendekati 50%.
2. Melakukan penelitian pembangkitan kode OTP dengan jumlah digit yang lebih banyak.
3. Proses implementasi OTP tidak hanya diterapkan pada teknologi website saja akan tetapi bisa diterapkan untuk sistem autentikasi *Smartphone*