BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari penelitian perbandingan generator kunci Logistic Map dan Henon Map terhadap algoritma Rijndael 256 bits yang sudah dimodifikasi, dan implementasi ke dalam aplikasi Live Chat berbasis web adalah sebagai berikut.

1. Protokol keamanan *live chat* ini sudah memenuhi beberapa spesifikasi keamanan dari kriptografi yaitu kerahasiaan, dan integritas data karena dapat melindungi pesan yang berupa data teks. Pesan akan tersimpan di dalam database dengan aman karena pesan yang tersimpan dalam bentuk enkripsi, dan telah diuji keamanan peretasannya dengan bantuan *software* Wireshark.
2. Dari penelitian yang sudah dilakukan maka disimpulkan bahwa dua generator kunci Logistic Map dan Henon Map menghasilkan nilai *avalanche effect* yang baik tergantung dari kombinasi kunci, baik itu numerik maupun alfanumerik.
3. Pada pengujian aplikasi live chat dengan serangan *man-in-the-middle-attack*, kriptanalis mencoba dengan cara *brute force attack*, dan memberikan hasil yang tidak mungkin terpecahkan. Sesuai dengan penelitian yang pernah dilakukan terdahulu bahwasannya suatu ciphertext yang dibangkitkan oleh algoritma Rijndael 256 bits dengan kemungkinan kunci memiliki kombinasi sebanyak 1.1×10^{77} dengan waktu yang dibutuhkan selama 3.31×10^{56} tahun untuk mencoba seluruh kemungkinan kunci. Dapat disimpulkan bahwa serangan brute force ini akan sangat banyak memakan waktu untuk mencoba semua kemungkinan.

5.2 Saran

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

1. Untuk penelitian selanjutnya, sebaiknya menambah generator kunci terhadap Algoritma Rijndael 256 bits yang telah dimodifikasi, atau melakukan pengujian terhadap keamanan live chat menggunakan teknik serangan lain selain brute force attack.
2. Bagi penelitian selanjutnya, sebaiknya menggunakan Henon Map jika masukan kunci berupa alfanumerik hal tersebut dikarenakan hasil dari penggunaan generator kunci Henon Map akan lebih baik tingkat keacakannya.
3. Untuk penelitian selanjutnya, implementasi Live Chat menggunakan Algoritma Rijndael 256 bits yang sudah dimodifikasi dapat diterapkan pada sistem live chat yang dilakukan oleh lebih dari dua user, seperti live chat grup.