BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari penelitian Modifikasi Algoritma Rijndael 256 *bits*, dan Implementasi dari Algoritma Rijndael 256 *bits* yang sudah di modifikasi, Algoritma RSA, dan fungsi hash SHA256 ke dalam aplikasi *Live Chat Customer Service* berbasis Web adalah sebagai berikut.

1. Algoritma Rijndael 256 *bits* yang telah dimodifikasi di bagian S-box dan ShiftRow telah diuji dengan menggunakan pengujiuan *Avalanche Effect* dan pengujian *Randomness Test.* Untuk pengujian *Randomness Test* hasil enkripsi berupa *ciphertext* berhasil lolos melalui beberapa opsi tes yang diberikan seperti *Frequency test, Poker Test, Run Test, Long Run Test,* dan *Serial Test*, karena semua hasil berada dibawah maximal test value, hal ini membuktikan barisan biner dari hasil ciphertext benar – benar acak.

   Pada hasil pengujian *avalanche effect* terlihat bahwa modifikasi dibagian ShiftRow lebih memberikan hasil yang lebih baik 50.2232 %, sedangkan hasil pengujian *avalanche effect* pada modifikasi bagian S-box memberikan hasil 48.9955 %. Jadi, modifikasi dibagian ShiftRow lebih memberikan hasil *avalanche effet* yang baik. Untuk pengujian *Avalanche Effect* dari semua aspek memberikan nilai sekitar 50.7813 %, dari penelitian yang sudah dilakukan maka disimpulkan bahwa algoritma ini sangat baik dan tahan terhadap kriptanalis. Salah satu cara untuk menghasilkan nilai *avalanche effect* yang baik juga tergantung dari kombinasi kunci, baik itu numerik atau alfanumerik.
2. Protokol keamanan *Live Chat* yang dibangun dengan Algoritma Rijndael 256 *bits* yang sudah di modifikasi dan dikombinasikan dengan Algoritma RSA dan fungsi hash SHA256 kedalam Aplikasi *Live Chat* berhasil di implementasikan. Protokol Keamanan di *live chat* ini sudah memenuhi beberapa aspek dari kriptografi yaitu kerahasiaan (*Confidentiality)* dan integritas data (*Data Integrity*) karena sudah dapat melindungi pesan anatara

customer dan *customer service* berupa data teks. Pesan juga akan tersimpan dengan aman karena pesan disimpan di database hanya pada saat *live chat* berlangsung, setelah *customer service* keluar dari sistem maka chat akan otomatis tersimpan pada log chat, dan masih dalam keadaan terenkripsi dan pesan bisa dikembalikan ke bentuk plainteks jika sewaktu – waktu pesan dibutuhkan.

3. Pengujian Aplikasi *Live chat* dengan serangan *man-in-the-middle-attact* mendapatkan pesan yang akan dikirim. Kriptanalis mencoba dengan cara *Exhaustive attack* atau *Brute force attack* dan memberikan hasil yang tidak mungkin terpecahkan karena membongkar suatu *ciphertext* yang dibangkitkan Rijndael 256 *bits*, kemungkinan kunci memiliki kombinasi sebanyak 1.1×10^{77} dengan waktu 3.31×10^{56} tahun. Jadi, serangan brute force akan banyak sekali memakan waktu untuk mecoba semua kemungkinan.
4. Untuk membuktikan pesan asli dikirim dari pengirim yaitu dengan cara memvalidasi nilai hash pesan sebelum pesan dikirimkan dan pesan sesudah dikirimkan, jika nilai hash sama maka tidak ada perubahan pada saat pengiriman data, jika nilai hash tidak sama maka pesan terjadi perubahan pada saat transmisi data.

5.2 Saran

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

1. Untuk penelitian selanjutnya modifikasi pada Algoritma Rijndael di dalam aplikasi matlab dapat melakukan enkripsi lebih dari 1 blok. Dan juga bisa dikombinasikan dengan algoritma kriptografi yang lain seperti RSA.
2. Untuk penelitian selanjutnaya, pada aplikasi *Live chat* dapat memberikan integritas data atau melindungi data per-*session.* Menambah pemberitahuan setiap ada pesan baru atau belum terbaca.