BAB V
PENUTUP

5.1. Kesimpulan

Berdasarkan hasil pengujian yang telah dilakukan, maka kesimpulan yang dapat diambil dari penelitian ini adalah:

1. Berkas pesan suara terenkripsi memiliki ukuran yang lebih besar daripada ukuran berkas pesan suara asli. Pada penelitian ini rata-rata kenaikan ukuran berkas suara terenkripsi sebesar 49,97%. Hal ini dikarenakan adanya penambahan *padding* pada blok yang kosong maupun untuk *integrity check* berkas pesan suara tersebut.
2. Berkas pesan suara terdekripsi memiliki ukuran yang sama dengan berkas suara asli. Hal dikarenakan algoritma AES merupakan algoritma kunci simetris, dimana kunci enkripsi yang digunakan sama dengan kunci dekripsinya.
3. Waktu proses enkripsi dan dekripsi berkas pesan suara tergantung dari besarnya ukuran berkas. Semakin besar ukuran berkas pesan suara, maka semakin lama waktu yang diperlukan.
4. Kecepatan rata-rata yang dihasilkan dari proses enkripsi berkas pesan suara sebesar 1,254 KB/detik, sedangkan kecepatan rata-rata untuk proses dekripsi 1,308 KB/detik.
5. Enkripsi pesan suara menggunakan algoritma AES ini terbukti mampu mengamankan pesan suara. Hal tersebut dibuktikan dengan hasil enkripsi 20 dari 20 pesan suara atau 100% pesan suara yang berubah menjadi suara *noise*.
6. Validitas isi pesan suara terdekripsi terhadap pesan suara asli tidak mengalami perubahan. Hal tersebut dibuktikan dengan hasil 20 dari 20 pesan suara terdekripsi atau 100 % pesan suara terdekripsi memiliki kesamaan isi dengan pesan suara asli.

5.2. Saran

Berdasarkan pengujian pada aplikasi kriptografi pesan suara menggunakan *Advanced Encryption Standard* ada beberapa saran untuk pengembangan lebih lanjut, yaitu:

1. Aplikasi kriptografi pesan suara menggunakan *Advanced Encryption Standard* ini hanya dapat memproses satu berkas pesan suara pada satu kali proses. Diharapkan dapat dikembangkan aplikasi yang mampu melakukan pemrosesan enkripsi maupun dekripsi untuk beberapa berkas dalam satu waktu pemrosesan.
2. Agar berkas pesan suara terenkripsi tidak mengalami kenaikan ukuran berkas yang cukup besar, dapat pula dikombinasikan dengan penambahan proses pemampatan *(compressing).*
3. Aplikasi kriptografi pesan suara menggunakan *Advanced Encryption Standard* ini dapat dikembangkan menggunakan bahasa pemrograman yang lain, sehingga mampu dijalankan di semua *platform.*
4. Penelitian ini dapat pula dikembangkan dengan implementasi pada sistem pengamanan *voicemail* IP PBX dan diukur kinerjanya.

DAFTAR PUSTAKA

Alyanto, D. (2016). *Penerapan Algoritma AES : Rijndael dalam Pengenkripsian Data Rahasia.* Medan: Sekolah Tinggi Manajemen Informatika dan Komputer TIME.

Ariyus, D. (2006). *Kriptografi: Keamanan Data Dan Komunikasi* (1 ed.). Yogyakarta: Penerbit Graha Ilmu.

Binanto, I. (2010). *MULTIMEDIA DIGITAL, Dasar Teori + Pengembangan.* Yogyakarta: Andi Offset.

Ibrahim, R. N. (2012). Kriptografi Algoritma DES, AES/Rijndael, Blowfish untuk Keamanan Citra Digital dengan Menggunakan Metode Discrete Wavelet. *Jurnal Computech & Bisnis, 6*(2), 82-95.

Khusnul, F. (2012). Implementasi Keamanan Pengiriman Pesan Suara dengan Enkripsi dan Deskripsi Menggunakan Algoritma Twofish. *Journal of Informatics and Technology, 1*(3), 84-89.

Kritoforus, R., & Aditya, S. (2012). Implementasi Algoritma Rijndael untuk Enkripsi dan Deskripsi pada Citra Digital. *Seminar Nasional Aplikasi Teknologi Informasi 2012.* Yogyakarta.

Munir, R. (2006). *Kriptografi*. Bandung: Penerbit Informatika.

NIST. (2001). *Fips-pub 197, advance encryption system (aes).* Retrieved Juli 20, 2017, from http://csrc.nist.gov/pubications/fips/fips197/fips-197.pdf

Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java.* Yogyakarta: Penerbit Andi.

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.). New York: John Wiley & Sons, Inc.

Setyaningsih, E. (2015). *Kriptografi & Implementasinya Menggunakan MATLAB.* Yogyakarta: Penerbit Andi.

Silva, L. D., Heriyanto, & Dessyanto. (2013). Aplikasi Enkripsi dan Deskripsi File dengan Menggunakan AES (Advanced Encryption Standard) Algoritma Rijndael pada Sistem Operasi Android. *Telematika, 10*(1), 33-42.