BAB I
PENDAHULUAN

1.1. Latar Belakang

Komunikasi suara merupakan komunikasi yang paling umum digunakan oleh pengguna sistem informasi. Salah satu media untuk komunikasi suara adalah melalui telepon. Salah satu fitur dasar pada sistem teleponi, seperti IP PBX, adalah pesan suara. Ketika nomor pesawat yang dituju sibuk atau tidak dijawab, maka penelepon bisa merekam pesan suara dan pesan suara tersebut tersimpan di *server* IP PBX. Format audio pada perekaman pesan suara secara umum adalah WAV, AMR, dan GSM.

Beberapa sistem IP PBX memungkinkan pesan suara yang ditinggalkan penelepon untuk diakses melalui protokol *web* atau http. Selanjutnya, pesan suara tersebut bisa diunduh maupun diteruskan melalui *email*. Untuk menjaga pesan suara tersebut dapat diakses oleh pengguna yang berhak, diperlukan sistem pengamanan data audio pesan suara tersebut.

Pengamanan terhadap data dapat dilakukan dengan berbagai cara, yaitu steganografi, *watermarking,* dan kriptografi. Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman (Schneier, 1996). Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah (Setyaningsih, 2015).

Atas dasar uraian tersebut, maka pada penelitian ini peneliti mengambil judul Kriptografi Pesan Suara Menggunakan Algoritma AES *(Advanced Encryption Standard).*

1.2. Rumusan Masalah

Rumusan masalah yang dapat didefinisikan dalam penelitian ini diantaranya adalah sebagai berikut:

1. Bagaimana melakukan enkripsi pesan suara menggunakan algoritma *Advanced Encryption Standard.*
2. Bagaimana melakukan dekripsi pesan suara yang sudah dilakukan kriptografi.
3. Bagaimana kinerja perangkat lunak kriptografi menggunakan algoritma *Advanced Encryption Standard.*

1.3. Batasan Masalah

Batasan masalah dalam penelitian Kriptografi Pesan Suara Menggunakan Algoritma AES *(Advanced Encryption Standard)* ini adalah sebagai berikut:

1. Berkas pesan suara yang digunakan hanya berkas berformat WAV.
2. Kunci yang digunakan pada proses enkripsi dan dekripsi berkas pesan suara hanya kunci dengan panjang 128 bit.
3. Aplikasi kriptografi yang dibangun menggunakan bahasa pemrograman PHP.

1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk mengimplementasikan algoritma *Advanced Encryption Standard* pada kriptografi berkas audio.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah terimplementasinya algoritma *Advanced Encryption Standard* pada sebuah sistem yang dapat membantu pengguna untuk melakukan enkripsi dan dekripsi pesan suara.