ABSTRAK

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 berkas pesan suara menggunakan algoritma *Advanced Encryption Standard.* Akuisisi berkas pesan suara sampel dilakukan dengan cara mengunduh berkas pesan suara pada IP PBX. Sampel pesan suara yang diambil sebanyak 20 berkas dengan ukuran berkas yang berbeda-beda. Setelah melakukan penginputan berkas audio, proses selanjutnya adalah mengenkripsi berkas audio tersebut. Proses enkripsi dimulai dengan mengubah berkas audio tersebut dalam bentuk heksadesimal dan masukan tersebut dikopikan ke dalam *state* kemudian dilanjutkan dengan proses transformasi *byte AddRoundKey* dengan struktur yang terdiri dari 4 proses yaitu *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey* secara berulang-ulang sebanyak Nr-1. *Round* yang terakhir agak berbeda dengan *round* sebelumnya di mana pada *round* terakhir tidak mengalami transformasi *MixColumns.* Pada AES-128 yang memiliki panjang kunci 16 *byte*, banyaknya *round* adalah 10. Seluruh fungsi operasi (perkalian dan penjumlahan) pada AES merupakan operasi yang didefinisikan menggunakan tabel substitusi dengan cara menginterpretasikan *byte* masukan menjadi dua bilangan heksadesimal.

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. Berkas pesan suara terdekripsi memiliki ukuran yang sama dengan berkas suara asli. 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. 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. 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. 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.

Kata Kunci: *Kriptografi, Voicemail, Advanced Encryption Standard*