ABSTRAK

Masalah keamanan dalam sistem komunikasi merupakan hal penting yang perlu diperhatikan, walaupun terkadang diabaikan karena dianggap mengurangi kenyamanan. Salah satu teknik pengamanan data adalah dengan kriptografi atau pengacakan dan penyusunan ulang pesan dengan algoritma tertentu agar pesan hanya dimengerti oleh pihak yang berhak. Algoritma AES-128 penulis gunakan untuk mengamankan komunikasi suara pada sistem fixed line telephone atau PSTN dengan pertimbangan kuat terhadap serangan-memerlukan kombinasi plaintext chipertext sebanyak 2^{127} kali untuk panjang kunci 128-bit, cepat-waktu pemrosesan singkat secara hardware dan software, dan bebas atau terbuka untuk digunakan.

Algoritma Rijndael-karya Rijmen dan Daemen dari Belgia-diumumkan sebagai *Advanced Encryption Standard* (AES) oleh *National Institute of Standards and Technology* (NIST) pada tahun 2001. Algoritma ini merupakan block cipher simetris (pengirim dan penerima menggunakan kunci yang sama) dengan panjang blok data 128-bit dan panjang kunci bervariasi antara 128-bit (AES-128), 192-bit (AES-129), dan 256-bit (AES-256)

Untuk implementasi sistem kriptografi suara ini memerlukan proses pengubahan sinyal analog ke digital dan sebaliknya, proses kompresi dan dekompresi sinyal digital untuk mengurangi besar bandwidth yang diperlukan, dan sistem prosesor 8-bit untuk aplikasi AES-128. Sistem prosesor 8-bit menggunakan varian dari Intel MCS-51 keluaran dari Atmel untuk aplikasi enkripsi dan dekripsi data *speech* dalam bentuk sinyal digital. Data terenkripsi ini dikirim menggunakan perantara modem melalui kanal PSTN antara pengirim dan penerima.