ABSTRAK

Voice over Internet Protocol (VoIP) adalah teknologi yang mampu melewatkan trafik suara, video dan data berbentuk paket melalui jaringan IP. Jaringan IP adalah jaringan komunikasi data yang berbasis *packet switch*. Dengan berkomunikasi menggunakan VoIP, keuntungan yang dapat diambil adalah biaya yang lebih murah dibandingkan tarif telepon konvesional.

VoIP menggunakan jaringan IP untuk melewatkan data suara. Jaringan IP sendiri merupakan jaringan publik, yang digunakan banyak pihak. Karakteristik jaringan publik adalah rawan terhadap *attackers*. Tingkat keamanan jaringan publik lebih buruk daripada jaringan privat.

Salah satu cara untuk mengamankan VoIP yaitu dengan melakukan enkripsi pada data suara hasil kompresi di server VoIP menggunakan algoritma kriptografi *stream cipher*. Di server VoIP penerima, data suara hasil enkripsi akan didekripsi untuk mendapatkan kembali suara asli. Data yang mengalir di jaringan IP adalah data suara hasil enkripsi, sehingga *attackers* membutuhkan kunci dekripsi dan algoritma kriptografi-nya untuk membongkar data suara tersebut. Salah satu algoritma *stream cipher* yang dapat digunakan adalah algoritma SEAL.

Jaringan VoIP sangat sensitif terhadap *delay*. ITU-T merekomendasikan maksimum *delay end-to-end* pada jaringan VoIP adalah 150 ms. Penambahan modul kriptografi pada server VoIP akan menambah *delay end-to-end*. Penambahan *delay end-to-end* tersebut diusahakan masih di bawah maksimum *delay end-to-end* yang direkomendasikan ITU-T.

Dari hasil penelitian diperoleh suatu kesimpulan bahwa dengan menambah modul kriptografi SEAL pada jaringan VoIP, delay end-to-end masih di bawah maksimum delay end-to-end yang direkomendasikan ITU-T. Data suara hasil enkripsi tidak mengeluarkan suara, sehingga paket data suara yang melewati jaringan IP sulit disadap.

Kata Kunci : jaringan IP, algoritma kriptografi, *delay end-to-end*, enkripsi, dekripsi