BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

VoIP atau dapat disebut juga sebagai *Voice over Internet Protocol*, merupakan protokol jaringan yang berfungsi untuk melakukan panggilan suara melalui jaringan IP (*Internet Protocol*) termasuk digitalisasi aliran suara (Cisco.com, 2016), dan VoIP sangat berbeda dari teknologi *telephone* konvensional. Transportasi media pada semua aplikasi multimedia, termasuk VoIP, menggunakan RTP (*Realtime Transport Protocol*) sebagai penghubung dengan UDP (*User Datagram Protocol*) (Goode, 2002). VoIP memiliki beberapa kelebihan, di antaranya adalah, VoIP akan menghemat biaya komunikasi dan VoIP memiliki biaya *maintenance* yang relatif lebih murah, walaupun pada tahap awal pembangunan akan mahal dan sulit (Porter, dkk., 2006).

Kekurangan VoIP selain mahal pada tahap awal pembangunan, juga pada dasarnya paket yang dikirimkan tidak dienkripsi. Dengan tidak dienkripsinya paket, maka salah satu masalah yang dapat terjadi adalah *Wiretapping. Wiretapping* menjadi masalah karena dapat mencuri data privasi seperti tanggal lahir, jenis kelamin, agama, bahkan IP *address* atau metadata, serta dapat mengambil informasi sensitif lainnya seperti, resep rahasia, data finansial, atau data militer (Hoven, dkk, 2016). Pada data yang dirilis oleh Angelos D. Keromytis (2010) pada laporan dengan judul "*Voice-over-IP Security*", 20% masalah penyerangan yang terjadi di sistem VoIP adalah *eavesdropping*, yang menempati posisi kedua setelah *Denial of Services. Eavesdropping* dan *wiretapping* memiliki tujuan yang sama yaitu, untuk merekam dan memonitor percakapan tanpa diketahui (Net Industries, 2017). Salah

satu cara melakukan *wiretapping* adalah, dengan melakukan ARP (*Address Resolution Protocol*) *spoofing* dan alat yang digunakan untuk menangkap data adalah Wireshark (Shaidani, 2015).

Masalah pada *wiretapping* dapat dicegah dengan melakukan enkripsi pesan yang dikirim dengan algoritma enkripsi yang tersedia, salah satunya adalah Salsa20. Salsa20 merupakan algoritma enkripsi *stream cipher* yang didesain oleh Daniel J. Bernstein (Bernstein, 2012). Enkripsi *stream cipher* memiliki kecepatan proses lebih cepat dibandingkan dengan *block cipher* (Paar dan Pelzl, 2010). Salsa20 sudah terbukti sesuai untuk diimplementasikan pada perangkat yang memiliki spesifikasi terbatas seperti perangkat bergerak (Irawan, dkk, 2014). *Stream cipher* masuk pada kategori kriptografi kunci simetris, dimana proses enkripsi dan dekripsi menggunakan satu kunci yang sama (Irawan, dkk, 2014). Jika dalam proses dekripsi memerlukan kunci yang sama maka distribusi kunci haruslah aman agar kunci tidak dengan mudah dibaca oleh pihak lain (Yashaswini, 2015). Kunci yang didistribusikan harus dienkripsi terlebih dahulu agar distribusi kunci menjadi aman. Dalam melakukan enkripsi kunci, digunakan algoritma enkripsi asimetris bernama RSA (Rivest-Shamir-Adleman) dengan panjang kunci 1024 bit, karena algoritma enkripsi RSA memiliki keamanan yang baik serta masih menjadi algoritma enkripsi kunci publik yang populer dan banyak digunakan (Wulansari, dkk., 2016), dan panjang kunci 768 *bit* telah berhasil dipecahkan pada penelitian yang dilakukan oleh Thorsten Kleinjung, dkk. dengan judul penelitian "*Factorization of a 768-bit RSA modulus"*.

RSA dapat juga direferensikan sebagai algoritma Rivest-Shamir-Adleman. RSA merupakan algoritma enkripsi asimetris yang sudah digunakan oleh

kebanyakan orang (Paar dan Pelzl, 2010). Algoritma enkripsi asimetris pada RSA menggunakan kunci publik, sehingga tidak perlu ada rahasia kunci untuk melakukan enkripsi (Pfleeger dan Lawrence, 2007). Pada perhitungan enkripsi dan dekripsi RSA, digunakan cara matematika *Fast Exponential Modulus Arithmetic* yang diberikan oleh aptitudefordummies untuk mempercepat waktu proses.

Penelitian ini memiliki perbedaan dengan penelitian yang telah dilakukan sebelumnya oleh Satrio Ajie Wijaya dengan judul "Pengamanan Jaringan VoIP Dengan Memanfaatkan Algoritma Stream Cipher A5" (Wijaya, 2007), dengan perbedaan yang terletak pada penggunaan algoritma enkripsi . Pada penelitian kali ini akan dibahas tentang implementasi algoritma enkripsi RSA 1024 dan Salsa20 dalam aplikasi VoIP. RSA 1024 akan berperan sebagai algoritma yang melakukan enkripsi data untuk pertukaran kunci Salsa20. Sedangkan kunci dari Salsa20 sendiri bertujuan untuk enkripsi dan dekripsi data suara atau percakapan pengguna.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalahnya adalah bagaimana cara melakukan implementasi algoritma enkripsi Salsa20 untuk mengirim pesan suara dan implementasi algoritma enkripsi RSA 1024 untuk pertukaran kunci Salsa20 pada aplikasi VoIP?

1.3 Batasan Masalah

Terdapat beberapa batasan masalah dalam penelitian ini, dengan batasan masalah tersebut didefinisikan sebagai berikut.

1. Pada penelitian ini digunakan ukuran blok kunci sebesar 1024-bit.
2. Implementasi menggunakan *platform* yang sama (PC - PC).
3. Aplikasi dibuat hanya untuk implementasi RSA 1024 dan Salsa20.

4. Aplikasi dibuat dalam bahasa C#.

1.4 Tujuan Penelitian

Berdasarkan pada rumusan masalah di atas, tujuan dari penelitian ini adalah untuk implementasi algoritma enkripsi Salsa20 untuk mengirim pesan suara, dan implementasi algoritma RSA 1024 untuk melakukan pengiriman kunci Salsa20 pada aplikasi komunikasi VoIP, agar distribusi kunci Salsa20 dan pengiriman suara tidak mudah dicuri dan disalahgunakan oleh penyadap.

1.5 Manfaat Penelitian

Hasil dari penelitian ini, baik arsitektur maupun hasil pengujian, dapat digunakan sebagai referensi dalam rancang bangun atau implementasi VoIP yang aman dan dapat dijadikan referensi untuk perkembangan penelitian selanjutnya.

1.6 Sistematika Penulisan Laporan Penelitian

Dalam laporan ini terdapat sistematika penulisan yang terdiri dari :

BAB I PENDAHULUAN

Bab ini merupakan pembukaan dari laporan yang terdiri dari, latar belakang masalah, rumusan masalah, batasan penelitian, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini merupakan penjelasan dari teori-teori yang berkaitan serta mendukung dalam penelitian ini, antara lain, VoIP, RTP, Public Key Cryptosystem, RSA, Stream Cipher, dan Salsa20.

BAB III METODE DAN PERANCANGAN APLIKASI

Dalam bab ini dijelaskan metode dan perancangan aplikasi yang dibangun terdiri dari analisis kebutuhan sistem, perancangan *server*, perancangan protokol RTP dan perancangan *client*.

BAB IV IMPLEMENTASI DAN UJI COBA

Dalam bab ini dijelaskan implementasi algoritma enkripsi pada aplikasi yang telah dibangun dan dalam uji coba dilakukan untuk menentukan apakah implementasi algoritma sudah sesuai, menentukan apakah suara berhasil didengar penyadap atau tidak, perbandingan *processing delay*, perbandingan *jitter* dan perbandingan *throughput*.

BAB V SIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan dari hasil penelitian yang telah dilakukan. Beserta saran untuk membantu mengembangkan aplikasi lebih lanjut.