IMPLEMENTASI ALGORITMA ENKRIPSI RSA DAN SALSA20 DALAM PENGIRIMAN DATA APLIKASI KOMUNIKASI BERBASIS VOIP

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom.)

Bodhi Jaya

13110110035

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN INFORMATIKA

UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG

2017

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI ALGORITMA ENKRIPSI

RSA DAN SALSA20 DALAM PENGIRIMAN

DATA APLIKASI KOMUNIKASI BERBASIS VOIP

Oleh

Nama	: Bodhi Jaya
NIM	: 13110110035
Program Studi	: Teknik Informatika
Fakultas	: Teknik dan Informatika

Tangerang, 21 Agustus 2017

Ketua Sidang,	Dosen Penguji,
Marcel Bonar Kristanda, S.Kom.,M.Sc.	Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, CEH
Dosen Pembimbing I,	Dosen Pembimbing II,
Hargyo Tri Nugroho I., S.Kom., M.Sc.	Dr. Ir. P. M. Winarno, M.Kom.

Mengetahui

Ketua Program Studi

Teknik Informatika,

Maria Irmina Prasetiyowati, S.Kom., M.T.

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya,

Nama : Bodhi Jaya

NIM : 13110110035

Program Studi : Teknik Informatika

Fakultas : Teknik dan Informatika

Menyatakan bahwa skripsi yang berjudul **"Implementasi Algoritma Enkripsi RSA dan Salsa20 Dalam Pengiriman Data Aplikasi Komunikasi Berbasis VoIP"** ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/ penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 21 Agustus 2017

Bodhi Jaya

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya laporan skripsi berjudul Implementasi Algoritma Enkripsi RSA Dan Salsa20 Dalam Pengiriman Data Aplikasi Komunikasi Berbasis VOIP dapat terselesaikan tepat pada waktunya.

Laporan skripsi ini merupakan salah satu syarat kelulusan sebagai mahasiswa untuk memperoleh gelar sarjana. Penulis juga tidak lupa mengucapkan terima kasih kepada:

1. Dr. Ninok Leksono, sebagai Rektor Universitas Multimedia Nusantara,
2. Maria Irmina Prasetiyowati, S.Kom, M.T. selaku ketua program studi teknik informatika Universitas Multimedia Nusantara.
3. Hargyo Tri Nugroho I., S.Kom., M.Sc., sebagai pembimbing dalam perancangan aplikasi dari awal hingga akhir dan laporan skripsi dan memberi banyak saran dan masukan, sehingga aplikasi dan laporan ini dapat terselesaikan tepat pada waktunya.
4. Dr. Ir. P. M. Winarno, M.Kom., sebagai pembimbing dalam perancangan aplikasi dari awal hingga akhir dan laporan skripsi dan memberi banyak saran dan masukan, sehingga aplikasi dan laporan ini dapat terselesaikan tepat pada waktunya.
5. Kedua orang tua dan keluarga yang telah memberikan bantuan berupa materi maupun semangat moral, agar tetap semangat dan menyelesaikan laporan skripsi tepat pada waktunya, dan

6. Semua rekan dan sahabat yang tidak bisa saya sebutkan namanya satu per satu, yang telah memberikan semangat dan bantuan agar laporan terselesaikan tepat pada waktunya.

Tangerang, 21 Agustus 2017

Bodhi Jaya

IMPLEMENTASI ALGORITMA ENKRIPSI RSA DAN SALSA20 DALAM PENGIRIMAN DATA APLIKASI KOMUNIKASI BERBASIS VOIP

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah berkembang cepat. Salah satu perkembangan teknologi informasi dan komunikasi adalah VoIP. VoIP merupakan servis *telephone* melalui *internet*. Salah satu masalah dalam VoIP adalah penyadapan. Dalam penyadapan, data komunikasi antar pengguna dapat dicuri dan bahkan dapat disalahgunakan oleh penyadap. Oleh karena itu diperlukan arsitektur yang aman agar kegiatan penyadapan dapat dicegah, dengan salah satunya adalah melakukan enkripsi pada percakapan menggunakan Salsa20 dan RSA dengan panjang kunci 1024 bit. Dalam aplikasinya, Salsa20 berfungsi untuk melakukan enkripsi pada suara, dan RSA 1024 berfungsi untuk enkripsi kunci Salsa20 pada proses pengiriman. Dari penelitian ini, didapatkan hasil bahwa isi kunci Salsa20 yang dikirim teracak dan suara yang dikirim juga teracak. Hasil dari percobaan menunjukkan bahwa kunci dan suara berhasil dienkripsi oleh Salsa20 dengan *processing delay* yang dapat diterima dengan pengiriman data adalah 23,07 ms dan penerimaan data 21,416 ms.

Kata kunci : RSA1024, Salsa20 , VoIP

RSA AND SALSA20 ENCRYPTION ALGORITHM IMPLEMENTATION ON DATA TRANSMISSION IN VOIP BASE COMMUNICATION APPLICATION

ABSTRACT

Information and communication technology development has grown rapidly. One among many examples of it is VoIP – telephone service through internet. However, VoIP might be prone to wiretapping, in which, the data being communicated between users could be stolen and can even misused by tapper. Therefore, safe architecture is required so that wiretapping can be prevented in one way with encryption in conversation with Salsa20 and RSA with 1024 bits key length. In this proposed architecture, RSA 1024 is used to encrypt the shared-key which later used by Salsa20 for voice encryption. The experiment result shows that both Salsa20's key and voice are succesfuly ciphered with acceptable processing delay – 23,07 ms on the sender side, 21,416 ms on the receiver side.

Keyword : RSA1024, Salsa20 ,VoIP

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR RUMUS