



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

**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 SALS20 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,



Marcel Bonar Kristanda, S.Kom.,M.Sc.

Dosen Penguji,



Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, CEH

Dosen Pembimbing I,



Hargyo Tri Nugroho I., S.Kom., M.Sc.

Dosen Pembimbing II,



Dr. Ir. P. M. Winarno, M.Kom.

Mengetahui

Ketua Program Studi
Teknik Informatika,



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

ii

UNIVERSITAS
MULTIMEDIA
NUSANTARA

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

iii
MULTIMEDIA
NUSANTARA

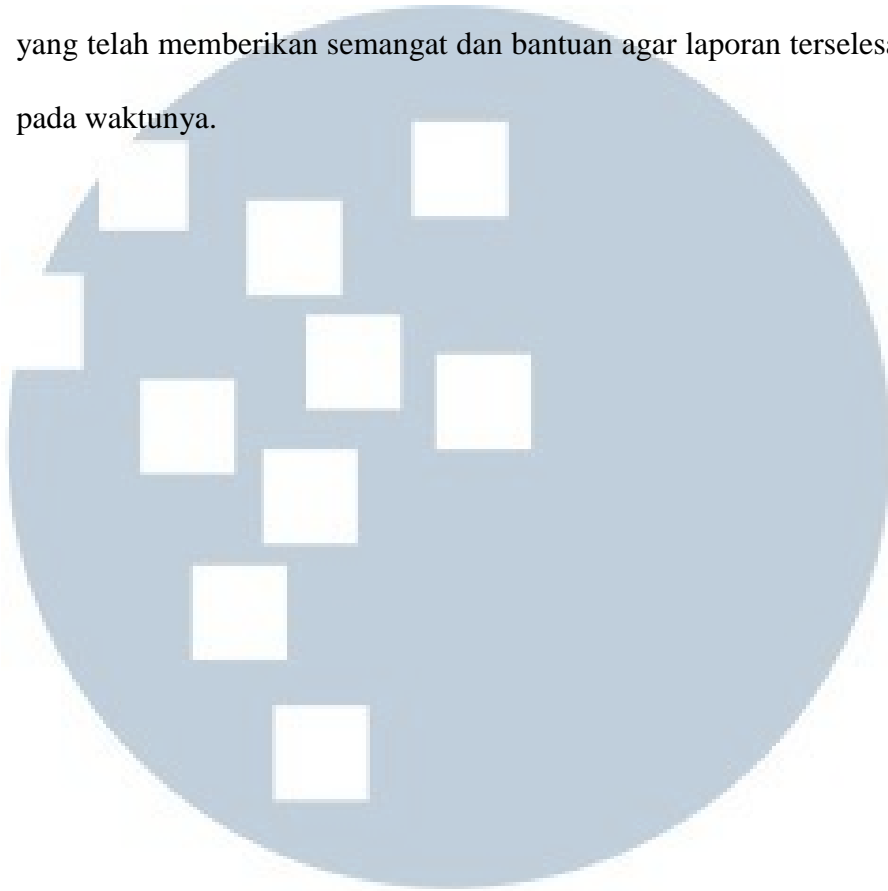
KATA PENGANTAR

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 Prasetyowati, 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.



UMMN

Tangerang, 21 Agustus 2017

UNIVERSITAS
MULTIMEDIA
NUSANTARA

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

UMMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

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 succesfully ciphered with acceptable processing delay – 23,07 ms on the sender side, 21,416 ms on the receiver side.

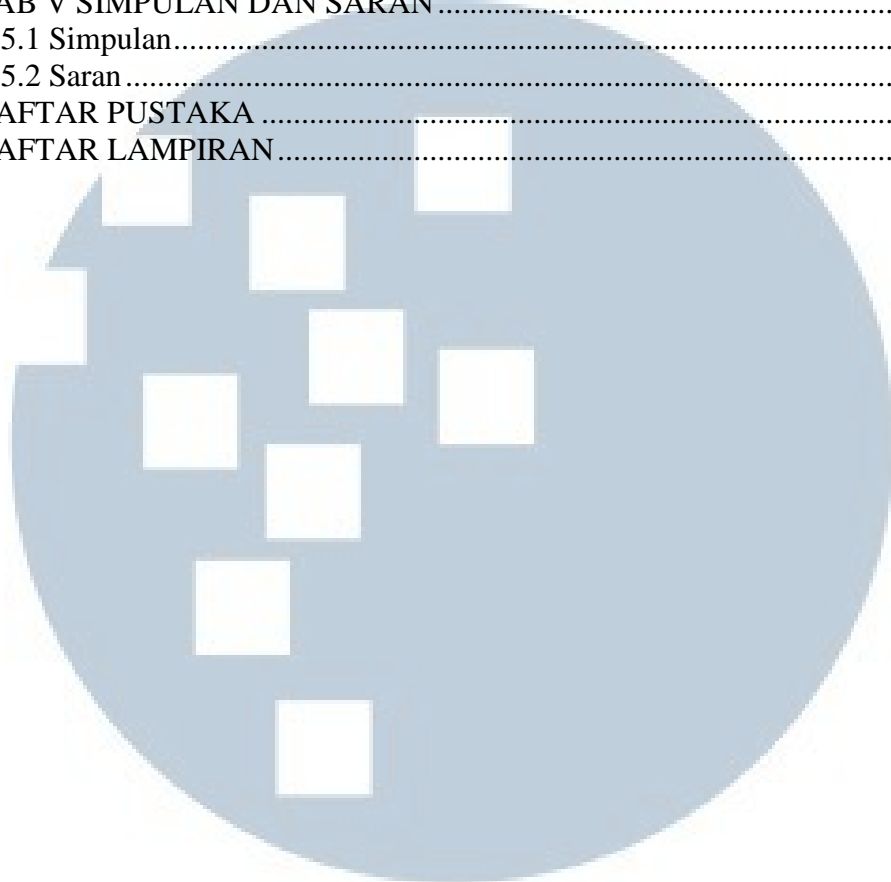
Keyword : RSA1024, Salsa20 ,VoIP



DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI	Error! Bookmark not defined.
PERNYATAAN TIDAK MELAKUKAN PLAGIAT	Error! Bookmark not defined.
KATA PENGANTAR	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR RUMUS	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan Laporan Penelitian	4
BAB II LANDASAN TEORI	6
2.1 VoIP (Voice over Internet Protocol)	6
2.2 RTP (Realtime Transport Protocol)	7
2.3 Public Key Cryptosystem	8
2.4 RSA (Rivest-Shamir-Adleman)	11
2.5 Stream Cipher	12
2.6 Salsa20	12
2.7 Jitter	14
2.8 ARP Spoofing	15
2.9 Fast Exponential Modulus Arithmetic	15
BAB III METODE DAN PERANCANGAN APLIKASI	17
3.1 Metode Penelitian	17
3.2 Perancangan Aplikasi	18
3.2.1 Analisis Kebutuhan Sistem	19
3.2.2 Data Flow Diagram	21
3.2.3 Flowchart	26
A. Flowchart Aplikasi Client	27
B. Flowchart Aplikasi Server	38
3.2.4 Struktur Tabel	41
BAB IV IMPLEMENTASI DAN UJI COBA	42
4.1 Spesifikasi Sistem	42
4.2 Implementasi	43
4.3 Uji Coba	49
4.3.1 Uji Coba Perhitungan Algoritma RSA 1024	51
4.3.2 Uji Coba Perhitungan Algoritma Salsa20	56
4.3.3 Uji Coba ARP Spoofing	57
4.3.4 Uji Coba Processing Delay	65
4.3.5 Uji Coba Perbandingan Jitter	68

4.3.6 Uji Coba Perbandingan Throughput	70
BAB V SIMPULAN DAN SARAN	72
5.1 Simpulan.....	72
5.2 Saran	73
DAFTAR PUSTAKA	74
DAFTAR LAMPIRAN.....	78



UMMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR GAMBAR

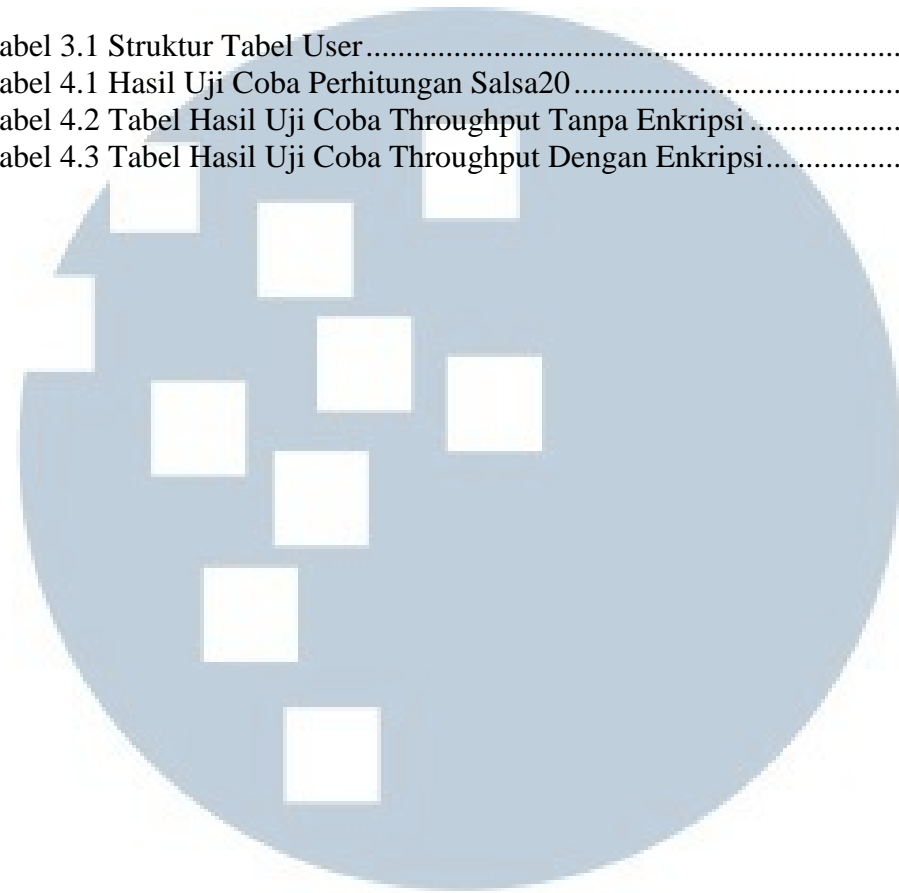
Gambar 2.1 Arsitektur Sederhana VoIP	6
Gambar 2.2 RTP Header	7
Gambar 2.3 Skema enkripsi menggunakan kunci publik	9
Gambar 2.4 Skema enkripsi menggunakan kunci pribadi	9
Gambar 2.5 Ilustrasi Proses Stream Cipher	12
Gambar 3.1 Context Diagram Program Utama.....	21
Gambar 3.2 DFD Level 1 Program.....	22
Gambar 3.3 DFD Level 2 Proses Login.....	24
Gambar 3.4 DFD Level 2 Proses Call.....	25
Gambar 3.5 Flowchart Alur Program	26
Gambar 3.6 Flowchart Main Client	27
Gambar 3.7 Flowchart Initialize	29
Gambar 3.8 Flowchart Command Listen	30
Gambar 3.9 Flowchart Command Invite.....	31
Gambar 3.10 Flowchart Command OK	32
Gambar 3.11 Flowchart Initializecall.....	33
Gambar 3.12 Flowchart Send.....	34
Gambar 3.13 Flowchart Receive.....	35
Gambar 3.14 Flowchart Login Aplikasi Client.....	36
Gambar 3.15 Flowchart Register	37
Gambar 3.16 Flowchart Call	38
Gambar 3.17 Flowchart Command Listen Aplikasi Server.....	39
Gambar 4.1 Tampilan Awal Aplikasi	43
Gambar 4.2 Proses Register	44
Gambar 4.3 Proses Login Salah	44
Gambar 4.4 Proses Login Berhasil.....	45
Gambar 4.5 Bagian Untuk Melakukan Panggilan.....	45
Gambar 4.6 Pengguna Melakukan Panggilan Ke Nomor Yang Dituju	46
Gambar 4.7 Pengguna Yang Dituju Tidak Ditemukan	47
Gambar 4.8 Mendapatkan Panggilan Dari Pengguna Lain.....	48
Gambar 4.9 Kondisi Menerima Panggilan.....	48
Gambar 4.10 Panggilan Berakhir.....	49
Gambar 4.11 Hasil Uji Coba RSA 1024 Skenario Pertama Aplikasi	53
Gambar 4.12 Hasil Uji Coba RSA 1024 Skenario Pertama Mobilefish	53
Gambar 4.13 Hasil Uji Coba RSA 1024 Skenario Kedua Aplikasi.....	54
Gambar 4.14 Hasil Uji Coba RSA 1024 Skenario Kedua Mobilefish.....	54
Gambar 4.15 Hasil Uji Coba RSA 1024 Skenario Ketiga Aplikasi.....	55
Gambar 4.16 Hasil Uji Coba RSA 1024 Skenario Ketiga Mobilefish.....	55
Gambar 4.17 Alamat IP sistem Pada Device Laptop.....	57
Gambar 4.18 Alamat IP Windows 7 Virtual Machine.....	57
Gambar 4.19 Alamat IP Ubuntu Linux Virtual Machine.....	58
Gambar 4.20 Ubuntu Linux Melakukan ARP Poisoning Ke Device Laptop	58
Gambar 4.21 Ubuntu Linux Melakukan ARP Poisoning Ke Windows 7 VM	59
Gambar 4.22 Host Windows 7 VM Berhasil Terkena ARP Poisoning	59
Gambar 4.23 Host Windows 7 Laptop Berhasil Terkena ARP Poisoning	60
Gambar 4.24 Penyadap Mulai Melakukan Capture Data.....	60

Gambar 4.25 Proses Register Device Laptop	61
Gambar 4.26 Proses Register Windows 7 Virtual Machine	61
Gambar 4.27 Proses Login Device Laptop	62
Gambar 4.28 Proses Login Windows 7 Virtual Machine	62
Gambar 4.29 Proses Melakukan Panggilan	63
Gambar 4.30 Kondisi Saat Dalam Menerima Panggilan	63
Gambar 4.31 Panggilan Telah Berakhir	64
Gambar 4.32 Memutar Suara Hasil Penyadapan	65
Gambar 4.33 Isi Paket Autentikasi Dari Aplikasi	65
Gambar 4.34 Hasil Perhitungan Processing delay Program Tanpa Enkripsi	66
Gambar 4.35 Delay Encoding Aplikasi Tidak Menggunakan Library	67
Gambar 4.36 Delay Decoding Aplikasi Tidak Menggunakan Library	67
Gambar 4.37 Rata - Rata Processing Delay Salsa20 Enkripsi dan Dekripsi	67
Gambar 4.38 Processing Delay Proses Enkripsi RSA 1024	67
Gambar 4.39 Processing Delay Proses Dekripsi RSA 1024	67
Gambar 4.40 Jitter Pada Aplikasi Tanpa Enkripsi	69
Gambar 4.41 Jitter Pada Aplikasi Dengan Enkripsi	69



DAFTAR TABEL

Tabel 3.1 Struktur Tabel User	41
Tabel 4.1 Hasil Uji Coba Perhitungan Salsa20	56
Tabel 4.2 Tabel Hasil Uji Coba Throughput Tanpa Enkripsi	70
Tabel 4.3 Tabel Hasil Uji Coba Throughput Dengan Enkripsi.....	71



UMMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR RUMUS

Rumus 2.1 Nilai n	11
Rumus 2.2 Nilai ϕ	11
Rumus 2.3 Nilai e	11
Rumus 2.4 Nilai d	11
Rumus 2.5 Enkripsi Pesan.....	11
Rumus 2.6 Dekripsi Pesan.....	11
Rumus 2.7 Rumus Enkripsi Stream Cipher.....	12
Rumus 2.8 Rumus Dekripsi Stream Cipher.....	12
Rumus 2.9 Fungsi Quarterround.....	13
Rumus 2.10 Fungsi Rowround.....	13
Rumus 2.11 Fungsi Columnround.....	14
Rumus 2.12 Perhitungan Jitter.....	14

UMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA