DAFTAR ISI

ABSTRAK i

ABSTRACT ii

KATA PENGANTAR iii

DAFTAR ISI v

DAFTAR TABEL x

DAFTAR GAMBAR xii

DAFTAR SIMBOL xv

DAFTAR LAMPIRAN xvi

BAB 1 PENDAHULUAN 1

1.1 Latar Belakang Masalah 1

1.2 Rumusan Masalah 2

1.3 Maksud dan Tujuan 2

1.3.1 Maksud 2

1.3.2 Tujuan 2

1.4 Batasan Masalah 3

1.5 Metodologi Penelitian 3

1.6 Sistematika Penulisan 4

BAB 2 TINJAUAN PUSTAKA 7

2.1 Jaringan Komputer 7

2.1.1 Jenis Jaringan Komputer 7

2.1.2 Arsitektur Jaringan Komputer 8

2.2 Protokol Jaringan Komputer 8

2.2.1 Model Referensi OSI 9

2.2.2 Protokol TCP/IP 13

2.2.2.1 Layanan TCP/IP 14

2.2.2.2 Arsitektur TCP/IP 15
2.2.2.3 Pengalamatan IP 18
2.3 Keamanan Jaringan Komputer 24
2.3.1 Tujuan Keamanan Jaringan Komputer 25
2.3.2 Tipe Ancaman Keamana Sistem Komputer 25
2.3.3 Bentuk Ancaman Jaringan Komputer 26
2.4 Konsep Dasar Algoritma 27
2.4.1 Sejarah Algoritma 27
2.4.2 Definisi Algoritma 28
2.5 Konsep Dasar Kriptografi 28
2.5.1 Sejarah Kriptografi 28
2.5.2 Pengenalan Algoritma Kriptografi 30
2.5.3 Macam Macam Algoritma Kriptografi 30
2.5.3.1 Algoritma Simetris (Konvensional) 31
2.5.3.2 Algoritma Asimetris 31
2.5.3.3 Fungsi Hash 32
2.6 Konsep Dasar Algoritma RSA 32
2.7 Voice Over IP 33
2.7.1 Protokol VoIP 36
2.7.1.1 *H.323* 36
2.7.1.2 *Real Time Protocol* (RTP) 37
2.7.1.2.1 Fitur yang Dimiliki 38
2.7.1.3 *Real-Time Control Protocol (RTCP)* 39
2.7.1.4 *Resource Reservation Protocol (RSVP)* 40
2.7.1.5 *Session Initiation Protocol* (SIP) 40
2.7.1.5.1 *Addressing* 41
2.7.1.5.2 *SIP Network Elements* 41
2.7.1.6 SRTP 50
2.7.2 Komponen dari *Voice-over-IP* 51
2.7.2.1 *Network Transport* 51
2.7.2.2 *Media Transport* 51

2.7.2.3 *Signaling* 52
2.7.2.3.1 *Dual Tone Multi Frequency (DTMF)* 52
2.7.2.4 *Directory Services* 53
2.7.2.5 Komponen Pendukung 54
2.7.2.5.1 *Media Encoding* 54
2.7.2.5.2 *Gateway Control* 55
2.7.3 Standar Kompresi Data Suara 55
2.7.3.1 G.711 56
2.7.3.2 G.723.1 56
2.7.4 Protocol Stack 57
2.7.5 VoIP *Gateway* 57
2.7.6 IP-PBX Server 58
2.8 *Advanced Encryption Standard* (AES) 58
2.9 ZRTP 59
2.9.1 *Key Agreement* 60
2.9.1.1 *Diffie Hellman* (DH) 60
2.9.1.2 *Preshared Mode* 63
2.9.1.3 Multistream Mode 63
2.9.2 ZRTP Messages 64
2.9.2.1 ZRTP *Message Format* 65
2.9.2.1.1 *Message Type Block* 65
2.9.2.1.2 *Hash Type Block* 66
2.9.2.1.3 *Cipher Type Block* 66
2.9.2.1.4 *Auth Tag Type Block* 67
2.9.2.1.5 *Key Agreement Type Block* 67
2.9.2.1.6 SAS *Type Block* 68
2.9.2.1.7 *Signature Type Block* 69
2.9.2.2 *Hello Message* 69
2.9.2.3 *HelloACK Message* 70
2.9.2.4 *Commit Message* 71
2.9.2.5 *DHPart1 Message* 74

2.9.2.6 *DHPart2 Message* 75
2.9.2.7 Confirm1 dan Confirm2 Messages 76
2.9.2.8 *Conf2ACK Message* 77
2.9.2.9 *Error Message* 77
2.9.2.10 *ErrorACK Message* 79
2.9.2.11 *GoClear Message* 79
2.9.2.12 *ClearACK Message* 80
2.9.2.13 *SASrelay Message* 80
2.9.2.14 *RelayACK Message* 81
2.9.3 *Short Authentication String (SAS)* 82
2.9.3.1 *SAS Verified flag* 82
2.9.3.2 Signing SAS 83
BAB 3 ANALISIS DAN PERANCANGAN 85
3.1 Analisis Sistem 85
3.1.1 Analisis Masalah 85
3.1.2 Analisis Metode Serangan 88
3.1.3 Analisa Short Authentication String (SAS) 91
3.1.4 Analisis Metode Pengamanan VoIP 95
3.1.5 Analisis ZRTP 95
3.1.6 Analisis VoIP Server 100
3.1.7 Analisis VoIP Client 102
3.1.8 Analisis Perangkat Keras 102
3.1.9 Analisis Perangkat Lunak 103
3.2 Perancangan Sistem 103
3.2.1 Tujuan Perancangan Sistem 103
3.2.2 Perancangan Aristektur 104
3.2.3 Perancangan Pengalamatan SIP ID 105
3.2.3.1 Perancangan SIP ID Pada *Server* 105
3.2.3.2 Perancangan SIP ID Pada *Client* 105
3.2.4 Perancangan Arsitektur Pengujian 106

BAB 4 IMPLEMENTASI DAN PENGUJIAN 109
4.1 Implementasi 109
4.1.1 Implementasi VoIP *Server* 109
4.1.1.1 Instalasi VoIP *Server* 110
4.1.1.2 Pembuatan SIP ID 111
4.1.2 Implementasi VoIP *Client* 113
4.1.2.1 Pendaftaran SIP ID 114
4.1.2.2 Konfigurasi ZRTP 116
4.2 Pengujian 117
4.2.1 Skenario Pengujian 118
4.2.2 Pengujian VoIP Server tanpa pengamanan 119
4.2.2.1 Pengujian Sebelum Komunikasi Berlangsung 119
4.2.2.2 Pengujian Pada Saat Komunikasi Berlangsung 124
4.2.3 Pengujian VoIP *Server* dengan pengamanan ZRTP 125
4.2.3.1 Pengujian sebelum komunikasi VoIP 125
4.2.3.2 Pengujian pada saat komunikasi VoIP berlangsung 128
4.2.4 Hasil Pengujian 130
BAB 5 KESIMPULAN DAN SARAN 131
5.1 Kesimpulan 131
5.2 Saran 131
DAFTAR PUSTAKA 133