DAFTAR ISI

ABSTRAK i

ABSTRACT ii

KATA PENGANTAR iii

DAFTAR ISI v

DAFTAR TABEL ix

DAFTAR GAMBAR x

DAFTAR SIMBOL xiv

DAFTAR LAMPIRAN xvii

BAB 1 PENDAHULUAN 1

1.1 Latar Belakang Masalah 1

1.2 Rumusan Masalah 2

1.3 Maksud dan Tujuan 2

1.4 Batasan Masalah 3

1.5 Metodologi Penelitian 3

1.5.1 Metode Pengumpulan Data 4

1.5.2 Metode Pembangunan Perangkat Lunak 4

1.6 Sistematika Penulisan 5

BAB 2 TINJAUAN PUSTAKA 7

2.1 VoIP (Voice Over Internet Protocol) 7

2.2 Manfaat Voip 7

2.2.1 Unsur Pembentuk Voip 7

2.2.1.1 *User Agent* 7
2.2.1.2 *Proxy* 8
2.2.1.3 *Protocol* 8
2.2.1.3.1 H.323 8
2.2.1.3.2 SIP (*Session Initiation Protocol*) 8
2.2.1.3.3 IAX (*The Inter-Asterisk Exchange*) 10
2.2.1.4 *Codec* 10
2.2.2 RTP (Realtime Treansfer Protocol) 11
2.2.3 SRTP (Secure Real Time Transport Protocol) 11
2.3 Kriptografi 12
2.3.1 Macam – Macam Algoritma Kriptografi 13
2.4 Algoritma Enkripsi AES 13
2.4.1 Rijndael Key Schedule 15
2.4.2 Proses Enkripsi AES 16
2.4.3 Proses Dekripsi AES 20
2.4.4 Counter Mode 23
2.5 Algoritma DES (*Data Encryption Standart*) 25
2.6 Algoritma *Triple* DES 26
2.7 Diffie-Hellman *key exchange* 27
2.8 Tools 29
2.8.1 Android 29
2.8.2 Java 31
2.8.3 Software Development Kit (SDK) 33

2.8.4 Linux 34
2.8.5 Asterisk 34
2.8.6 Android Studio 35
2.8.7 *Unified Modelling Language* (UML) 36
2.8.7.1 *Use Case Diagram* 36
2.8.7.2 *Activity Diagram* 36
2.8.7.3 *Class Diagram* 37
2.8.7.4 *Sequence Diagram* 38
BAB 3 ANALISIS DAN PERANCANGAN 39
3.1 Analisis Sistem 39
3.1.1 Analisis Masalah 39
3.1.2 Analisis SIP Dan RTP 40
3.1.3 Analisis Metode Serangan 41
3.1.4 Analisis Algoritma Kriptografi 41
3.1.5 Analisis SRTP 42
3.1.5.1 Analisis Algoritma AES-CTR 44
3.1.5.1.1 Proses Enkripsi 44
3.1.5.1.2 Proses Dekripsi 57
3.1.6 Analisis Arsitektur Sistem Yang Akan Dibangun 65
3.1.7 Analisis Diffie-Hellman *Key Exchange* 68
3.2 Spesifikasi Perangkat Lunak 69
3.2.1 Analisis Kebutuhan Non Fungsional 70
3.2.1.1 Analisis Kebutuhan Perangkat Lunak 70

3.2.1.2 Analisis Kebutuhan Perangkat Keras 70
3.2.1.3 Analisis Kebutuhan Pengguna 71
3.2.2 Analisis Kebutuhan Fungsional 71
3.2.2.1 Use Case Diagram 72
3.2.2.2 Use case scenario 72
3.2.2.3 Activity Diagram 74
3.2.2.4 *Class Diagram* 77
3.2.2.5 Sequence Diagram 79
3.3 Perancangan Sistem 81
3.3.1 Perancangan Struktur Menu 81
3.3.2 Perancangan Antarmuka Sistem 82
3.3.3 Perancangan Pesan 86
3.3.4 Jaringan Semantik 86
BAB 4 87
4.1 Implementasi 87
4.1.1 Implementasi VoIP *Server* 87
4.1.1.1 Instalasi VoIP *Server* 87
4.1.1.2 Pembuatan SIP ID 89
4.1.2 Implementasi *Class* 91
4.1.3 Implementasi VoIP *Client* 92
4.1.3.1 Pendaftaran SIP ID Pada *SSipCall* 92
4.1.3.2 Pendaftaran SIP ID Pada Aplikasi *Lindphone* 94
4.1.3.3 Konfigurasi *Secure Call* 95

4.1.3.3.1 Konfigurasi *SSipCall* 95
4.1.3.3.2 Konfigurasi *Linphone* 96
4.1.4 Implementasi Antarmuka..... 97
4.2 Pengujian 97
4.2.1 Skenario Pengujian..... 98
4.2.1.1 Pengujian Sistem VoIP Tanpa Menggunakan *Secure Call*..... 98
4.2.1.2 Pengujian Sistem VoIP Dengan Menggunakan *Secure Call* 100
4.2.1.3 Hasil Pengujian..... 102
BAB 5 103
5.1 Kesimpulan..... 103
5.2 Saran..... 103
DAFTAR PUSTAKA 104