DAFTAR ISI

LEMBAR PENGESAHAN

ABSTRAK ……...…… ii

ABSTRACT ……...……..…….. iii

KATA PENGANTAR ….....…...…….……. iv

DAFTAR ISI .....……...……...……. vi

DAFTAR GAMBAR ……...……...… xiii

DAFTAR TABEL ……...… xvi

DAFTAR SIMBOL ……..……..……...… xvii

BAB I PENDAHULUAN……...…..…… 1

1.1 Latar Belakang …… 1

1.2 Identifikasi Masalah …… 3

1.3 Maksud dan Tujuan …..……...…… 3

1.4 Batasan Masalah ……..... 4

1.5 Metodologi Penelitian …..…… 5

1.5.1 Metode Pengumpulan Data ...……...….…..... 5

1.5.2 Metode Pembuatan Perangkat Lunak ....……..…….…… 5

1.6 Sistematika Penulisan …..…… 7

BAB II LANDASAN TEORI……...…...…….. 9

2.1 *Electronic Mail* …… 9

2.1.1 Pengertian *Electronic Mail* ...…….……...…..... 9

2.1.2 Sistem Pengiriman E-mail.…….… 11

2.1.3 Protokol dan Standar E-Mail …… 13

2.1.3.1 Internet Message Format (IMF) ……..……... 14

2.1.3.2 Simple Mail Transport Protocol (SMTP)……..…… 15

2.1.3.3 Post Office Protocol ……..…..…… 16

2.1.4 Komponen E-Mail …….. 19

2.1.4.1 Envelope ……... 19

2.1.4.2 Header ……... 20

2.1.4.3 Body ……...……... 20

2.2 Jaringan Komputer ……...……..... 20

2.2.1 Dasar Arsitektur Jaringan Komputer …… 22

2.2.1.1 Local Area Network (LAN) ……..…….... 22

2.2.1.2 Metropolitan Area Network (LAN) ……..…….... 23

2.2.1.3 Wide Area Network (LAN) ……..…….... 23

2.2.1.4 Internet ……..…..……..... 23

2.2.1.5 Jaringan Tanpa Kabel (Wireless Network) …...…..... 24

2.2.2 Topologi Jaringan Komputer ……... 24

2.2.2.1 Topologi Bus ……...…...……..... 24

2.2.2.2 Topologi Token Ring …..…… 25

2.2.2.3 Topologi Star ……..... 26

2.2.2.4 Topologi Peer to Peer …….. 26

2.2.3 Protokol Jaringan Komputer …....……...……..……..... 27

2.3 Keamanan Jaringan Komputer ……..…...…..……..... 28

2.3.1 Aspek Keamanan Jaringan Komputer ……...……. 29

2.3.1.1 Privacy / Confidentiality ……..…..……..….……..... 29

2.3.1.2 Integrity …….. 30

2.3.1.3 Authentication …….……... 30

2.3.1.4 Availability …….……... 31

2.3.1.5 Access Control ……...…….……... 31

2.3.1.6 Non Repudiation ……... 32

2.3.2 Klasifikasi Keamanan Jaringan Komputer ……..……. 32

2.3.2.1 Keamanan Bersifat Fisik (*Physical Security*) ……..... 32

2.3.2.2 Keamanan Berhubungan dengan Orang (*Personel*) ….. 33

2.3.2.3 Keamanan Data dan Media Komunikasi……..….…..... 33

2.3.2.4 Keamanan dalam Operasi …...…..……..…….…..... 33

2.3.3 *Firewalls* ……....……...……. 34

2.3.3.1 Teknologi Penyaringan Paket (*Filtering Packets*) …..... 35

2.3.3.2 Teknologi *Gateway Layer* Aplikasi atau *Proxy* ……..... 35

2.3.3.3 Teknologi Inspeksi Keseluruhan Kondisi ……..... 36

2.3.4 Autentifikasi *Password* ……..……. 36

2.4 Kriptografi Menggunakan Algoritma CAST-128 …….……..... 37

2.4.1 Deskripsi Algoritma …..…….……..……...……. 39

2.4.2 Pasangan Kunci Putaran (*Pair of Round Keys*) .....…..……. 40

2.4.3 Putaran Tidak Identik (*Non-Identical Rounds*)……..……. 40

2.4.4 Kotak Operasi Subsitusi (*Substitution Boxes*)..…….…… 41

2.4.5 Penjadwalan Kunci (*Key Schedule*) ……...……. 41

2.4.6 Penyembunyian Kunci dan Rotasi Kunci ……....……. 43

2.4.7 Ukuran Kunci Penentu (*Variable Keysize*) ..……..…… 43

2.5 Rekayasa Perangkat Lunak ..……..…….……..... 44

2.5.1 Model Proses Pembuatan Perangkat Lunak ….…….……..……. 45

2.5.2 Metode Proses Pembuatan Perangkat Lunak …….…...…..……. 48

2.6 Perangkat Lunak Pendukung .…….……..... 50

2.6.1 Borland Delphi..……..…..……. 50

2.6.2 MDaemon ……...……..…..……. 51

2.6.3 Ethereal ……..…..……. 52

BAB III ANALISIS DAN PERANCANGAN SISTEM ….....……. 53

3.1 Analisis Masalah ……..…… 53

3.2 Analisis Sistem …...…….……..... 54

3.3 Kebutuhan Sistem …….…..... 56

3.3.1 Perangkat Keras …….……....…….. 56

3.3.2 Perangkat Lunak …….……...……....……. 57

3.4 Analisis Perangkat Lunak …….…..... 57

3.4.1 Proses Kriptografi ……..……....……. 57

3.4.1.1 Deskripsi Proses Enkripsi CAST-128 ……..……..…..... 59

3.4.1.2 Pasangan Kunci Putaran (*Pair of Round Keys*) .....…. 62

3.4.1.3 Putaran Tidak Identik (*Non-Identical Rounds*)……. 62

3.4.1.4 Kotak Operasi Subsitusi (*Substitution Boxes*)..……...…. 63

3.4.1.5 Penjadwalan Kunci (*Key Schedule*) ……....…. 63

3.4.1.6 Penyembunyian Kunci dan Rotasi Kunci ……...……. 65

3.4.1.7 Ukuran Kunci Penentu (*Variable Keysize*) …….……. 65

3.4.1.8 Deskripsi Proses Dekripsi CAST-128 ……...……. 66

3.4.2 Proses Pengiriman dan Penerimaan Pesan ……..……...……. 66

3.4.3 Manajemen *File* ……...……...……. 76

3.4.4 Manajemen dan Distribusi Kunci ……...……. 76

3.5 Perancangan Sistem …….……..... 78

3.5.1 Diagram Alir Perancangan Sistem ……...……...……. 79

3.5.2 Diagram Konteks ……..……...……...……. 82

3.5.3 *Data Flow Diagram* (DFD) Level 0 …...…….……. 83

3.5.4 Perancangan Struktur Menu Perangkat Lunak …...…….……. 86

3.5.5 Perancangan Antar Muka Perangkat Lunak ……...…….……. 87

3.5.5.1 Perancangan Antar Muka Daftar *Account* Baru ……..... 87

3.5.5.2 Perancangan Antar Muka Form Login ……..…..... 88

3.5.5.3 Perancangan Antar Muka Form Utama …….…..... 89

3.5.5.4 Perancangan Antar Muka Form Tulis Pesan …….…..... 90

3.5.5.5 Perancangan Antar Muka Form *Address Book* ….…..... 91

3.5.5.6 Perancangan Antar Muka Form *Security* (Enkripsi) 92

3.5.5.7 Perancangan Antar Muka Form *Security* (Dekripsi) 92

3.5.5.8 Perancangan Antar Muka Form *Password Generator* 93

3.5.5.9 Laporan Status ……..... 93

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM ..……....……. 94

4.1 Implementasi Sistem …...…..…….……..…….…….....…..... 94

4.1.1 Lingkungan Implementasi ….…..…...…….……...……...……. 94

4.1.2 Implementasi antar muka (*User Interface*) ….....…...…...…..…. 95

4.1.2.1 Tampilan antar muka Layar Pembuka 95
4.1.2.2 Tampilan antar muka Login 96
4.1.2.3 Tampilan antar muka *Form* Utama 97
4.1.2.4 Tampilan antar muka *Form Address Book* 97
4.1.2.5 Tampilan antar muka *Form* Tulis Pesan 98
4.1.2.6 Tampilan antar muka *Form Security* (Enkripsi) 99
4.1.2.7 Tampilan antar muka *Form* Laporan Proses Enkripsi berhasil 100
4.1.2.8 Tampilan antar muka Laporan Proses Pengiriman berhasil 101
4.1.2.9 Tampilan antar muka *Form* Baca Isi Pesan 101
4.1.2.10 Tampilan antar muka *Form Security* (Dekripsi) 103
4.1.2.11 Tampilan antar muka *Form Password Generator* 103
4.1.2.12 Tampilan antar muka Laporan Proses Dekripsi berhasil 104
4.2 Pengujian Sistem 105
4.2.1 Rencana Pengujian..... 105
4.2.2 Kasus Pengujian..... 105
4.2.2.1 Daftar *Account* 105
4.2.2.2 Login 107
4.2.2.3 Tulis Pesan 108
4.2.2.4 Baca Pesan 108
4.2.2.5 Security Enkripsi dan Dekripsi 110
4.2.2.6 Hasil Enkripsi 111

4.2.2.7 Hasil Dekripsi ……..……...……..... 111

4.2.3 Hasil Pengujian.……..……..…… 112

4.2.3.1 Input *file* (*attach*) untuk proses enkripsi ……..... 112

4.2.3.2 Output *file* (*attach*) hasil enkripsi ……..……..... 115

4.2.3.3 Pengujian pada Pesan tidak terenkripsi ..…..……..... 117

4.2.3.4 Pengujian pada Pesan terenkripsi ……...…..……..... 118

4.2.3.5 Pengujian pada *plaintext* kunci terenkripsi …..……..... 119

4.2.3.6 Kesimpulan hasil pengujian *blackbox* ……..... 120

4.2.3.7 Hasil Kuesioner Pengguna ……..……..……..... 121

BAB V KESIMPULAN DAN SARAN ……..…….....……. 121

5.1 Kesimpulan ……..……..... 125

5.2 Saran ….....….…..……..……..... 126

DAFTAR PUSTAKA

LAMPIRAN-LAMPIRAN

DAFTAR GAMBAR

Gambar 1.1	Diagram Watefall ……..……	6
Gambar 2.1	E-Mail Dalam Internet Menggunakan Mail Server ……...……	10
Gambar 2.2	Sistem Pengiriman Surat ……..……...……	11
Gambar 2.3	Komponen Konseptual Sistem E-Mail ……...……	12
Gambar 2.4	Sampling E-Mail *Header* yang ditetapkan oleh RFC 2822 ...…	14
Gambar 2.5	SMTP Mengidentifikasi *client* dan Penerima ……..……...……	16
Gambar 2.6	Otentifikasi Dasar dengan POP3 ……...……	18
Gambar 2.7	Penggunaan SMTP dan POP3 ……..……...……	18
Gambar 2.8	Jaringan Sederhana ……..……...……	21
Gambar 2.9	Topologi Bus ……..……..……...……	25
Gambar 2.10	Topologi Token Ring ……..……..……...……	25
Gambar 2.11	Topologi Star ……..……..……...……	26
Gambar 2.12	Topologi Peer to peer ……..……..……...……	26
Gambar 2.13	Layer OSI ……...…..……...……	27
Gambar 2.14	Layer TCP/IP ……..……..……...……	28
Gambar 2.15	Kriptografi Simetri dan Asimetri ……...……...……	38
Gambar 2.16	Diagram Waterfall ……..……..……...……	48
Gambar 2.17	Analisis Terstruktur .....……..……...……	50
Gambar 3.1.a	*Flowchart* Sistem pada *User* 1 (Pengirim) ……..……...……	55

Gambar 3.2.b *Flowchart* Sistem pada *User* 2 (Penerima) .....……..…… 55

Gambar 3.2 *Flowchart* Proses Enkripsi pada Aplikasi yang Dibangun ...… 58

Gambar 3.3 *Flowchart* Proses Dekripsi pada Aplikasi yang Dibangun ...… 59

Gambar 3.4 Alur Proses Enkripsi CAST-128 pada putaran ketiga……..... 61

Gambar 3.5 Proses Pengiriman dan Penerimaan Pesan ……...… 67

Gambar 3.6 *Flowchart* Proses Enkripsi dan Dekripsi Kunci ……..... 77

Gambar 3.7 Diagram Alir Proses Daftar *Account* baru ……...… 79

Gambar 3.8 Diagram Alir Proses Proses Pengiriman Pesan ……...… 80

Gambar 3.9 Diagram Alir Pembacaan Pesan ……..……...… 81

Gambar 3.10 Diagram Konteks Sistem E-Mail …….……...… 82

Gambar 3.11 DFD Level 0 ……...… 83

Gambar 3.12 DFD Level 1 Proses 1 ...……...… 85

Gambar 3.13 Perancangan Struktur Menu …….……...… 86

Gambar 3.14 Pendaftaran Form Daftar *Account* baru ……...… 87

Gambar 3.15 Form Login…..……..……...… 88

Gambar 3.16 Form Utama Aplikasi……...… 89

Gambar 3.17 Form Tulis Pesan……..……...… 90

Gambar 3.18 Form Address Book…...……...… 91

Gambar 3.19 Proses *Security* (Enkripsi) …….……...… 92

Gambar 3.20 Proses *Security* (Dekripsi) …….……...… 92

Gambar 3.21 Form Password Generator …….……...… 93

Gambar 3.22 Form Laporan Status …….……...… 93

Gambar 4.1 Tampilan Daftar *Account* MailForce……..……..... 96

Gambar 4.2 Tampilan Login MailForce……..……..……..... 96

Gambar 4.3 Tampilan Form Utama MailForce……..……..... 97

Gambar 4.4 Tampilan Form Address Book ...…….……..……..... 98

Gambar 4.5 Tampilan Form Tulis Pesan MailForce……..……..... 99

Gambar 4.6 Tampilan Form *Security* (Enkripsi) MailForce ……...…..... 100

Gambar 4.7 Tampilan Form Laporan Proses Enkripsi berhasil ...…...…..... 100

Gambar 4.8 Tampilan Form Laporan Proses Pengiriman berhasil .....…..... 101

Gambar 4.9 Tampilan Form Baca Isi Pesan Biasa ……...…..... 102

Gambar 4.10 Tampilan Form Baca Isi Pesan terenkripsi ……..... 102

Gambar 4.11 Tampilan Form Security (Dekripsi) MailForce……..... 103

Gambar 4.12 Tampilan Password Generator …….....…….....104

Gambar 4.13 Form Laporan Proses Dekripsi berhasil ……...…….....104

Gambar 4.14 Logo_unikom.bmp ……....……...…..... 112

Gambar 4.15 Tampilan hasil pengujian pesan tidak terenkripsi ...…….….... 118

Gambar 4.16 Tampilan hasil pengujian pesan terenkripsi ……...…..... 119

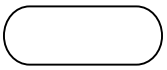
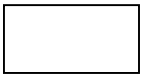
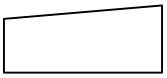
Gambar 4.17 Tampilan hasil pengujian plaintext kunci terenkripsi …….….... 120

DAFTAR TABEL

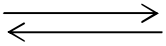
Tabel 4.1	Rencana Pengujian Aplikasi *Mail Client* ……...……..	105
Tabel 4.2	Pengujian Daftar *Account* ……...……...……..	106
Tabel 4.3	Pengujian Login ……...……...……...……..	107
Tabel 4.4	Pengujian Tulis Pesan ……..……...……...……..	108
Tabel 4.5	Pengujian Baca Pesan ……...…...……...……..	109
Tabel 4.6	Pengujian Security ……..……...……..	110
Tabel 4.7	Hasil Enkripsi ……...……...……...……..	111
Tabel 4.8	Hasil Dekripsi ……...……...……...……..	111

DAFTAR SIMBOL

1. Simbol *FlowChart*

NO	SIMBOL	KETERANGAN
1		Mulai / Selesai
2		Data
3		Proses
4		Penyimpanan Data
5		Dokumen
6		Aliran Data
7		Input Manual

2. Simbol *Data Flow Diagram* (DFD)

NO	SIMBOL	KETERANGAN
1		Proses
2		Terminator
3		Aliran Data
4		*Data Store*