DAFTAR ISI

LEMBAR JUDUL

LEMBAR PENGESAHAN

ABSTRAK. i

ABSTRACT ii

KATA PENGANTAR iii

DAFTAR ISI vi

DAFTAR TABEL xi

DAFTAR GAMBAR xii

DAFTAR SIMBOL xiv

DAFTAR LAMPIRAN xv

BAB I PENDAHULUAN

1.1 Latar Belakang 1

1.2 Identifikasi Masalah 2

1.3 Maksud dan Tujuan 3

1.4 Batasan Masalah 3

1.5 Metodologi Penelitian.. 4

1.5.1. Metode Penelitian..... 4

1.5.2. Metode Pengumpulan Data.. 4

1.5.3. Metode Pengembangan Perangkat Lunak.. 6

1.6 Sistematika Penulisan..... 7

BAB II TINJAUAN PUSTAKA

2.1 Pengertian Kriptografi 8

2.2 Dasar Matematis 9

2.3 Jenis Kriptografi 11

2.4 Algoritma RSA (*Rivest-Shamir-Adleman*) 13

2.5 Enkripsi dan Dekripsi 15

2.5.1 Enkripsi 15

2.5.2 Dekripsi 15

2.6 Konsep dasar Perhitungan Matematis 15

2.6.1 Fungsi Phi-Euler 15

2.6.2 Algoritma Euclide 16

2.6.2.1 Algoritma Euclide diperluas 16

2.6.3 Metode Fast Exponentiation 17

2.7 Proses Algoritma RSA 18

2.7.1 Pembentukan Kunci 18

2.7.2 Enkripsi RSA 19

2.7.3 Dekripsi RSA 20

2.8 Pengertian Jaringan Komputer 20

2.8.1 Jenis-jenis Jaringan Komputer 20

2.8.2 Topologi Jaringan Komputer 23

2.8.3 Manfaat Jaringan Komputer 25

2.9 *Visual Basic* 28

2.9.1 Sejarah Singkat *Visual Basic* 28

2.9.2 IDE *Visual Basic* 29
2.9.3 Jendela IDE 30
2.9.4 Jenis File Pada *Visual Basic* 34
2.9.5 Komponen Pada *Visual Basic* 34
2.10 Pendekatan rekayasa Perangkat Lunak 36
2.10.1 Pengertian Rekayasa Perangkat Lunak 36
2.10.2 Model Proses *Waterfall* (pressman 1992) 37
2.11 *Flowchart* 39
BAB III ANALISIS DAN PERANCANGAN
3.1 Analisis Masalah 41
3.1.1 Gambaran umu Sistem 42
3.1.2 Contoh Proses Enkripsi dan Dekripsi RSA 43
3.2 Analisis Non Fungsional 45
3.2.1 Analisis Kebutuhan Sistem 45
3.2.1.1 Analisis Kebutuhan Perangkat Keras 46
3.2.1.2 Analisis Kebutuhan Perangkat Lunak 47
3.2.1.3 Analisis Jaringan 48
3.2.1.4 Analisis Pengguna 49
3.3 Analisis Masukkan dan Keluaran Sistem 50
3.4 Analisis Proses Algoritma RSA 50
3.4.1 Proses Pembentukan Kunci Pada Algoritma RSA 51
3.4.2 Proses Enkripsi Menggunakan RSA 51
3.4.3 Proses Dekripsi Menggunakan RSA 52

3.4.4 Konversi Plainteks ke Bilangan Sequent 52
3.5 Analisis Fungsional 53
3.5.1 Diagram Konteks 53
3.5.2 Data Flow Diagram 55
3.5.3 Spesifikasi Proses 56
3.5.4 Kamus Data 58
3.6 Perancangan Sistem 59
3.6.1 Perancangan Prosedural 60
3.6.2 Bagan Alir Sistem 62
3.6.3 Diagram Alir Aplikasi KomDat LAN 62
3.7 Perancangan Struktur Menu 64
3.8 Perancangan Tampilan Antara Muka (*interface design*) 65
3.9 Jaringan Semantik 71
BAB IV IMPLEMENTASI DAN PENGUJIAN
4.1 Implementasi Sistem 72
4.1.1 Perangkat Keras 72
4.1.2 Perangkat Lunak 73
4.1.3 Implementasi Aplikasi 73
4.2 Pengujian Sistem 78
4.2.1 Skenario Pengujian 78
4.2.1.1 Pengujian Koneksi 79
4.2.1.2 Pengujian Kirim Pesan Teks 80
4.2.1.3 Pengujian Kirim File Teks 80

4.2.1.4 Pengujian Terima Pesan Teksi 81

4.2.1.5 Pengujian Terima File Teks 81

4.2.2 Analisa Hasil Pengujian Alpha 83

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan..... 84

5.2 Saran..... 84

DAFTAR PUSTAKA