

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
LEMBAR PENGESAHAN	iii
LEMBAR PENGESAHAN PENGUJI SIDANG	iv
LEMBAR PERNYATAAN	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
ABSTRAKSI	xiv
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Perumusan Masalah.....	3
1.3. Pembatasan Masalah.....	3
1.4. Tujuan dan Manfaat.....	4
1.5. Metode Penelitian.....	5
1.6. Sistematika Penulisan.....	5
BAB II LANDASAN TEORI	7
2.1. Pembuatan.....	7
2.2. Aplikasi.....	7
2.3. Algoritma.....	7
2.4. Kriptografi.....	8
2.5. Aspek – aspek keamanan.....	9
2.6. Macam - Macam Algoritma Kriptografi.....	11
2.7. Cryptanalysis.....	13

2.7.1.	Macam – macam serangan Cryptanalysis	15
2.8.	Kriptografi Kunci Public	17
2.8.1.	Konsep Kriptografi Kunci-Public	18
2.8.2.	Sejarah Kriptografi Kunci-Public.....	19
2.8.3.	Perbandingan Kriptografi Kunci-Simetri dan Kriptografi Kunci-Public	21
2.9.	Algoritma Kriptografi Kunci – Public	22
2.9.1.	RSA	22
2.9.1.1	Perumusan Algoritma RSA.....	23
2.9.1.2	Algoritma Membangkitkan Pasangan Kunci.....	25
2.9.1.3	Algoritma Enkripsi / Dekripsi	27
2.9.2.	El Gamal	29
2.9.3.	Knapsack.....	30
2.10.	Protocol Kriptografi.....	30
2.10.1.	Fungsi Protocol.....	31
2.10.2.	Penyerangan terhadap protocol.....	32
2.10.3.	Berbagai macam basic cryptanalytic attacks.....	33
2.11.	Flowchart.....	36
2.12.	Visual C# .NET	38
2.12.1.	Arsitektur Framework .NET	38
2.12.2.	Arsitektur Visual .NET	39
2.12.3.	Keuntungan Visual C #.....	40
BAB III METODOLOGI PENELITIAN		41
3.1	Metode Penelitian	41
3.2	Tempat dan Waktu Penulisan	42
3.3	Tahapan Penelitian.....	42
3.4	Alat dan Bahan	42

BAB IV ANALISIS DAN PEMBAHASAN	44
4.1 Analisis Kebutuhan.....	44
4.2 Gambaran Umum Aplikasi	45
4.3 Prinsip Kerja Aplikasi.....	46
4.3.1 Algoritma Kriptografi RSA.....	48
4.3.2 Perhitungan Algoritma RSA	53
4.4 Metode Perancangan Aplikasi	55
4.4.1 Flowchart Proses Utama	55
4.4.2 Flowchart Proses Enkripsi	56
4.4.3 Flowchart Proses Dekripsi	57
4.5 Perancangan Aplikasi	58
4.6 Algoritma Aplikasi	60
4.6.1 Tahap Encrypting.....	60
4.6.1.1 Fungsi Pembuatan Kunci	60
4.6.1.2 Fungsi Encrypt Data.....	61
4.6.2 Tahap Decrypting.....	62
4.6.2.1 Fungsi Decrypt Data	62
4.7 Implementasi	63
4.7.1 Implementasi Proses Encrypting.....	64
4.7.2 Implementasi Proses Decrypting.....	65
4.8 Evaluasi	66
4.8.1 Tipe Data	66
4.8.2 Halaman Utama	66
4.8.3 Halaman Generate Key	67
4.8.4 Menu E ncrypt File	70
4.8.5 Menu Decrypt File	75
4.8.6 About	80

BAB V	KESIMPULAN DAN SARAN.....	81
5.1	Kesimpulan.....	81
5.2	Saran.....	81

DAFTAR PUSTAKA

DAFTAR RIWAYAT HIDUP

LAMPIRAN

DAFTAR TABEL

Tabel 4.1	Hasil Uji Coba	81
-----------	----------------------	----

DAFTAR GAMBAR

	Halaman
Gambar 2.1	Proses enkripsi dan dekripsi..... 9
Gambar 2.2	Proses enkripsi-dekripsi algoritma kriptografi simetri 11
Gambar 2.3	Proses enkripsi-dekripsi algoritma asimetri 12
Gambar 2.4	Komposisi bahasa C#.....38
Gambar 2.5	Arsitektur Visual C# .NET40
Gambar 4.1	Prinsip kerja enkripsi47
Gambar 4.2	Prinsip kerja dekripsi48
Gambar 4.3	Skema Proses Algoritma Asimetri.....50
Gambar 4.4	Skema Proses Enkripsi dan Dekripsi dalam Algoritma Kriptografi RSA.....51
Gambar 4.5	Diagram alur Proses Enkripsi dan Dekripsi52
Gambar 4.6	Flowchart Proses Utama56
Gambar 4.7	Flowchart Proses Enkripsi57
Gambar 4.8	Flowchart Proses Dekripsi57
Gambar 4.9	Struktur Program59
Gambar 4.10	Form Utama.....67
Gambar 4.11	Form Generate Key.....68
Gambar 4.12	Proses penyimpanan kunci private.....69
Gambar 4.13	Proses penyimpanan kunci public.....69
Gambar 4.14	Menu Proses Encrypt File.....70
Gambar 4.15	Proses pengambilan kunci public.....74
Gambar 4.16	Proses Pesan yang terenkripsi75
Gambar 4.17	Proses pengambilan kunci private.....79
Gambar 4.18	Tampilan About Program80