

TAKARIR

Kriptografi	Suatu ilmu atau seni mengamankan pesan/data.
Kriptografer	Orang yang mengamankan pesan/data
Kriptanalisis	Ilmu atau seni untuk membuka keamanan data
Kriptanalis	Orang yang membuka keamanan data
RSA	Salah satu metode kriptografi kunci publik (asimetris)
Plainteks	Data yang bisa dibaca
Cipherteks	Data yang tidak bisa dibaca
Enkripsi	Merubah plainteks menjadi cipherteks dengan kunci tertentu
Dekripsi	Merubah cipherteks menjadi plainteks
Privat key	Kunci yang dimiliki oleh pribadi untuk melakukan dekripsi
Publik key	Kunci yang diberikan kepada orang lain (umum) untuk melakukan enkripsi
Simetris	Kunci yang digunakan untuk mengenkripsi dan mendekripsi adalah sama
Asimetris	Kunci yang digunakan untuk mengenkripsi dan mendekripsi adalah kunci yang berbeda tetapi merupakan pasangan
Bilangan Prima	Bilangan yang hanya mempunyai 2 faktor pembagi yaitu 1 dan bilangan itu sendiri
Mod (modulo)	Sisa hasil bagi
GCD	Greatest Common Divisor (Faktor pembagi bersama terbesar)
Autentikasi	Keaslian data/pcsan
Digital Signatur	Tanda tangan digital
User	Pemakai atau pengguna program aplikasi
Input	Masukan
Output	Keluaran
Interface	Tampilan program aplikasi
Flash screen	Tampilan awal yang akan hilang ketika menu utama ditampilkan

DAFTAR ISI

JUDUL	i
LEMBAR PENGESAHAN PEMBIMBING	ii
LEMBAR PENGESAHAN PENGUJI	iii
HALAMAN PERSEMBAHAN	iv
HALAMAN MOTTO	v
KATA PENGANTAR	vi
ABSTRAKSI	ix
TAKARIR	x
DAFTAR ISI	xi
DAFTAR GAMBAR	xiv
DAFTAR TABEL	xv
BAB I PENDAHULUAN	i
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Metode Penelitian	5
1.6.1 Pengumpulan Data	5
1.6.2 Pembuatan Sistem	5
1.7 Sistematika Penulisan	6
BAB II LANDASAN TEORI	8
2.1 Kriptografi	8
2.2 Algoritma Kriptografi	10
2.2.1 Algoritma Simetris	10
2.2.2 Algoritma Asimetris	11
2.3 Algoritma RSA	12
2.3.1 Landasan Matematis untuk Algoritma RSA	13
2.3.1.1 Bilangan Prima	13
2.3.1.2 Aritmetika Modulus	15
2.3.1.3 Faktor Pembagi Bersama Terbesar	16
2.3.1.4 Invers Modulo	16
2.3.1.5 Teorema Fermat	17
2.3.1.6 Teorema Euler	18
2.3.1.7 Bukti Matematis RSA	19
2.3.2 Enkripsi dan Dekripsi Menggunakan RSA	21
2.3.3 Autentifikasi	21
2.3.4 Perhitungan Matematis Algoritma RSA	22
BAB III ANALISIS KEBUTUHAN PERANGKAT LUNAK	24
3.1 Kebutuhan Analisis	24

3.2	Metode Analisis	24
3.3	Langkah-langkah Analisis Sistem	25
3.4	Hasil Analisis	25
3.4.1	Analisis Masukan	25
3.4.2	Analisis Keluaran	26
3.4.3	Analisis Antarmuka	26
3.4.4	Analisis Fungsi	27
3.4.5	Kebutuhan Perangkat Lunak	28
BAB IV	PERANCANGAN PERANGKAT LUNAK	29
4.1	Metode Perancangan	29
4.2	Rancangan Proses	29
4.3	Perancangan Algoritma RSA	30
4.3.1	Perancangan Pembangkitan Kunci RSA	30
4.3.2	Perancangan Proses Enkripsi RSA	33
4.3.3	Perancangan Proses Dekripsi RSA	35
4.4	Perancangan Antarmuka	37
BAB V	IMPLEMENTASI PERANGKAT LUNAK	40
5.1	Implementasi Secara Umum	40
5.2	Batasan Implementasi	40
5.2.1	Bahasa Yang Dipakai	40
5.2.2	Lingkungan Pengembangan	41
5.2.3	Batasan-batasan yang Digunakan	41
5.3	Implementasi Antarmuka	42
5.3.1	Flash Screen	42
5.3.2	Interface Menu Utama	43
5.3.3	Interface Pembangkitan Kunci	44
5.3.4	Interface Enkripsi dan Dekripsi File	45
5.3.5	Interface Enkripsi dan Dekripsi Teks	46
5.3.6	Interface Informasi Tentang Algoritma RSA	47
5.3.7	Interface Informasi Tentang Program	48
BAB VI	ANALISIS KINERJA PERANGKAT LUNAK	49
6.1	Penanganan Kesalahan	49
6.2	Analisis Pembangkitan kunci	50
6.3	Analisis Input	51
6.3.1	Input Enkripsi file atau Folder	51
6.3.2	Input Enkripsi Teks	51
6.4	Analisis Output	52
6.4.1	Output Enkripsi File	52
6.4.2	Output Enkripsi Teks	53
6.5	Analisis Perbandingan	54
6.5.1	Analisis Perbandingan Waktu Proses	54
6.5.2	Analisis Perbandingan Penggunaan Memori	57
6.5.3	Analisis Perbandingan Ukuran File	58

6.6 Kelebihan dan Kekurangan	60
6.7 Analisis Keamanan Algoritma RSA.....	61
BAB VII PENUTUP	62
7.1 Kesimpulan	62
7.2 Saran	63
DAFTAR PUSTAKA	64



DAFTAR GAMBAR

Gambar 2.1. Proses Enkripsi/Dekripsi Sederhana	9
Gambar 2.2. Proses Enkripsi/Dekripsi kriptografi kunci publik	12
Gambar 4.1. Proses enkripsi dan dekripsi menggunakan publik key dan privat key	30
Gambar 4.2. Flowchart pembangkitan kunci RSA	32
Gambar 4.3. Flowchart proses enkripsi RSA	34
Gambar 4.4. Flowchart proses Dekripsi RSA	36
Gambar 4.5. Rancangan form menu utama	37
Gambar 4.6. Rancangan form pembangkitan kunci	38
Gambar 4.7. Rancangan form enkripsi/dekripsi teks	38
Gambar 4.8. Rancangan form enkripsi/dekripsi file	39
Gambar 5.1. Proses inisialisasi bilangan prima	42
Gambar 5.2. Antarmuka menu utama	44
Gambar 5.3. Antarmuka pembangkitan kunci	45
Gambar 5.4. Antarmuka enkripsi file atau folder.	46
Gambar 5.5. Antarmuka konfigurasi.	46
Gambar 5.7. Antarmuka enkripsi teks	47
Gambar 5.8. Antarmuka informasi tentang algoritma RSA	48
Gambar 5.9. Antarmuka informasi tentang program	48
Gambar 6.1. Penanganan kesalahan pada dekripsi teks	49
Gambar 6.2. Pesan peringatan waktu pembangkitan kunci	50
Gambar 6.3. Pesan informasi waktu untuk proses enkripsi file.	52
Gambar 6.4. Hasil enkripsi teks.	53
Gambar 6.5. Diagram perbandingan waktu proses enkripsi (dalam detik)	55
Gambar 6.6. Diagram waktu proses dekripsi (dalam detik).....	56
Gambar 6.7. Diagram perbandingan pemakaian memori (dalam KB)	58
Gambar 6.8. Diagram perbandingan perubahan ukuran file hasil enkripsi.	59