

ABSTRAK

Tujuan dari Tugas Akhir ini adalah untuk membuat aplikasi dalam mengenkripsi dan mendekripsikan suatu data dalam bentuk pesan atau gambar. Teknik-teknik yang digunakan adalah McEliece, Elgamal, dan Rabin. Aplikasi berjudul “John’s Encryption-Decryption”

Pengguna dapat menyandikan pesan maupun gambar dengan teknik – teknik kunci-publik tertentu, yakni : Elgamal, McEliece, dan Rabin. Setelah disandikan maka pengguna dapat menyimpan hasil kodenya tersebut di dalam bentuk *file*. Untuk mengembalikannya ke pesan asli, pengguna hanya cukup mengambil *file* yang sebelumnya pernah di simpan agar dapat melakukan dekripsi.

Pengguna dapat melihat hasil perbandingan dari tiap teknik. Efisiensi yang dimaksud terdiri dari waktu, ukuran file, dan banyaknya karakter di setiap file. Pengguna juga dapat melihat diagram batang dari perbandingan efisiensi setiap teknik.

kata kunci : McEliece, Elgamal, Rabin, Enkripsi, Dekripsi, Sandi, Kunci-Publik, Efisiensi

ABSTRACT

The aim of this last task is to be capable of making the application in encrypting and decrypting to encode data to form a message or picture, using McEliece's, ElGamal's, and Rabin's technique. The application is John's Encryption-Decryption.

Users are able to encode either message or picture using the certain public technique key which are ElGamal, McEliece and Rabin. After Encoding, the user are able to save the code in the file form. And turning back the original message is just to take the files which have been saved before to make decryption.

User can be able to know and see the result of comparison from every technique. With the efficiency of time, size of file and the character in every file. Either see the comparison efficiency from the rectangle diagram from every technique.

keyword : McEliece, Elgamal, Rabin, Encrypting, Decrypting, Encoding, Public-Key, Efficiency.

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS.....	ii
SURAT PERNYATAAN ORISINALITAS KARYA	iii
KATA PENGANTAR	iv
ABSTRAK.....	vi
ABSTRACT	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xiv
DAFTAR TABEL.....	xvi
DAFTAR CUPLIKAN KODE PROGRAM	xvii
DAFTAR LAMPIRAN	xviii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan	2
1.4 Ruang Lingkup Proyek	3
1.5 Definisi, Akronim, dan Singkatan	3
1.6 Overview Laporan	4
1.7 Gambaran Keseluruhan	6
1.7.1 Perspektif Produk.....	6
1.7.2 Fungsi Produk.....	6
1.7.3 Karakteristik Pengguna.....	7
1.7.4 Batasan – Batasan	7
1.7.5 Asumsi Ketergantungan	7
1.8 Time Schedule	8
BAB II SPESIFIKASI PRODUK	9
2.1 Persyaratan Antarmuka Eksternal.....	9
2.1.1 Antarmuka dengan Pengguna.....	9

2.1.2 Antarmuka Perangkat Keras	9
2.1.3 Antarmuka Perangkat Lunak	9
2.1.4 Antarmuka Komunikasi	10
2.2 Fitur Produk Perangkat Lunak	10
2.2.1 Fitur 1 Enkripsi Pesan Rabin	11
2.2.1.1 Tujuan	11
2.2.1.2 Urutan Stimulus	11
2.2.1.3 Persyaratan Fungsional yang Berhubungan	11
2.2.2 Fitur 2 Enkripsi Pesan ElGamal	11
2.2.2.1 Tujuan	11
2.2.2.2 Urutan Stimulus	12
2.2.2.3 Persyaratan Fungsional yang Berhubungan	12
2.2.3 Fitur 3 Enkripsi Pesan McEliece	12
2.2.3.1 Tujuan	12
2.2.3.2 Urutan Stimulus	12
2.2.3.3 Persyaratan Fungsional yang Berhubungan	13
2.2.4 Fitur 4 Enkripsi Gambar Rabin	13
2.2.4.1 Tujuan	13
2.2.4.2 Urutan Stimulus	13
2.2.4.3 Persyaratan Fungsional yang Berhubungan	14
2.2.5 Fitur 5 Enkripsi Gambar ElGamal	14
2.2.5.1 Tujuan	14
2.2.5.2 Urutan Stimulus	14
2.2.5.3 Persyaratan Fungsional yang Berhubungan	14
2.2.6 Fitur 6 Enkripsi Gambar McEliece	15
2.2.6.1 Tujuan	15
2.2.6.2 Urutan Stimulus	15
2.2.6.3 Persyaratan Fungsional yang Berhubungan	15
2.2.7 Fitur 7 Dekripsi Pesan Rabin	16
2.2.7.1 Tujuan	16
2.2.7.2 Urutan Stimulus	16

2.2.7.3 Persyaratan Fungsional yang Berhubungan	16
2.2.8 Fitur 8 Dekripsi Pesan ElGamal	17
2.2.8.1 Tujuan	17
2.2.8.2 Urutan Stimulus	17
2.2.8.3 Persyaratan Fungsional yang Berhubungan	17
2.2.9 Fitur 9 Dekripsi Pesan McEliece	18
2.2.9.1 Tujuan	18
2.2.9.2 Urutan Stimulus	18
2.2.9.3 Persyaratan Fungsional yang Berhubungan	18
2.2.10 Fitur 10 Enkripsi Gambar Rabin	18
2.2.10.1 Tujuan	19
2.2.10.2 Urutan Stimulus	19
2.2.10.3 Persyaratan Fungsional yang Berhubungan	19
2.2.11 Fitur 11 Dekripsi Gambar ElGamal	19
2.2.11.1 Tujuan	20
2.2.11.2 Urutan Stimulus	20
2.2.11.3 Persyaratan Fungsional yang Berhubungan	20
2.2.12 Fitur 12 Dekripsi Gambar McEliece	20
2.2.12.1 Tujuan	20
2.2.12.2 Urutan Stimulus	20
2.2.12.3 Persyaratan Fungsional yang Berhubungan	21
2.2.13 Fitur 13 Save hasil Enkripsi / Dekripsi	21
2.2.13.1 Tujuan	21
2.2.13.2 Urutan Stimulus	21
2.2.13.3 Persyaratan Fungsional yang Berhubungan	22
2.2.14 Fitur 14 Load pesan asli / hasil enkripsi	22
2.2.14.1 Tujuan	22
2.2.14.2 Urutan Stimulus	22
2.2.14.3 Persyaratan Fungsional yang Berhubungan	22
2.2.15 Fitur 15 Perbandingan Algoritma	23
2.2.15.1 Tujuan	23

2.2.15.2 Urutan Stimulus	23
2.2.15.3 Persyaratan Fungsional yang Berhubungan	23
BAB III DESAIN PERANGKAT LUNAK.....	24
3.1 Dasar Teori	24
3.1.1 Kriptografi (cryptography)	24
3.1.2 Algoritma Kriptografi.....	26
3.1.3 Algoritma Simetris	27
3.1.4 Algoritma Asimetris (Public-Key Algorithm)	28
3.1.5 Algoritma Elemen dari Enkripsi.....	31
3.1.6 Kunci yang digunakan dan panjangnya kunci.....	33
3.1.7 Teori Matematika.....	34
3.1.7.1 Bilangan Bulat	34
3.1.7.2 Bilangan Prima.....	35
3.1.7.3 Algoritma Extended Euclidean.....	35
3.1.7.4 Matriks Invers	36
3.1.7.5 Hamming Code	38
3.1.7.6 Matriks Permutasi.....	38
3.1.8 Algoritma ElGamal	42
3.1.8.1 Prosedur Membuat Pasangan Kunci	43
3.1.8.2 Enkripsi	44
3.1.8.3 Dekripsi	44
3.1.8.4 Contoh Perhitungan Enkripsi Elgamal	45
3.1.9 Algoritma Rabin.....	50
3.1.9.1 Prosedur Membuat Pasangan Kunci	50
3.1.9.2 Enkripsi	51
3.1.9.3 Dekripsi	51
3.1.9.4 Contoh Perhitungan Enkripsi Rabin.....	52
3.1.10 Algoritma McEliece.....	54
3.1.10.1 Prosedur Membuat Pasangan Kunci	55
3.1.10.2 Enkripsi	55
3.1.10.3 Dekripsi	55

3.1.10.4 Contoh Perhitungan Enkripsi McEliece	56
3.1.11 Identifikasi	60
3.1.12 Overview Sistem	61
3.2 Keputusan Desain Perangkat Lunak Secara Keseluruhan	61
3.2.1 Use Case Diagram	61
3.2.2 Activity Diagram	64
3.3 User Interface Design.....	80
3.4 Class Diagram.....	94
3.5 Class Definition	95
3.5.1 Class MAIN	95
3.5.2 Class ElGamal_E_T_FRM	95
3.5.3 Class ElGamal_D_T_FRM	95
3.5.4 Class ElGamal_E_P_FRM	96
3.5.5 Class ElGamal_D_P_FRM	96
3.5.6 Class McEliece_E_T_FRM.....	96
3.5.7 Class McEliece_D_T_FRM	97
3.5.8 Class McEliece_E_P_FRM	97
3.5.9 Class McEliece_D_P_FRM	97
3.5.10 Class Rabin_E_T_FRM.....	97
3.5.11 Class Rabin_D_T_FRM.....	98
3.5.12 Class Rabin_E_P_FRM.....	98
3.5.13 Class Rabin_D_P_FRM	98
3.5.14 Class Loading_FRM	99
3.5.15 Class Efeciency_FRM	99
3.5.16 Class GEN_CHECK_PRIME	99
3.5.17 Class POWER_MOD	100
3.5.18 Class Image_Converter.....	100
3.5.19 Class MATRIKS_GEN.....	100
3.5.20 Class HammingCode	100
3.5.21 Class EXTENDED_EUCLIDEAN.....	101
BAB IV PENGEMBANGAN SISTEM	102

4.1 Perencanaan Tahap Implementasi.....	102
4.1.1 Pembagian Class	102
4.1.2 Keterkaitan antar Class	102
4.2 Perjalanan Tahap Implementasi	119
4.2.1 Top Down Implementasi.....	119
4.2.2 Error Handling	120
4.2.3 Ulasan Realisasi Fungsionalitas.....	120
4.2.4 Ulasan Realisasi User Interface Design	122
BAB V TESTING DAN EVALUASI SISTEM.....	136
5.1 Rencana Pengujian Sistem Terimplementasi	136
5.1.1 Test Case.....	136
5.1.2 Uji Fungsionalitas Modul/Class.....	140
5.2 Perjalanan Metodologi Pengujian	140
5.2.1 Black Box	140
5.2.2 White Box.....	147
5.3 Ulasan Hasil Evaluasi.....	152
BAB VI KESIMPULAN DAN SARAN	153
6.1 Keterkaitan antara Kesimpulan dengan Hasil Evaluasi.....	153
6.2 Keterkaitan antara Saran dengan Hasil Evaluasi.....	153
6.3 Rencana Perbaikan / Implementasi terhadap Saran yang Diberikan.....	154
DAFTAR PUSTAKA.....	xix
LAMPIRAN DATA PENULIS.....	xx

DAFTAR GAMBAR

Gambar III.1 Skema algoritma simetris	28
Gambar III.2 Skema algoritma asimetris	29
Gambar III.3 Pengelompokan enkripsi beserta contoh.....	31
Gambar III.4 Diagram Use Case.....	61
Gambar III.5 Activity Diagram Pembangkit Kunci Manual Rabin	65
Gambar III.6 Activity Diagram Pembangkit Kunci Otomatis Rabin	66
Gambar III.7 Activity Diagram Pembangkit Kunci Manual McEliece	67
Gambar III.8 Activity Diagram Pembangkit Kunci Otomatis McEliece	68
Gambar III.9 Activity Diagram Pembangkit Kunci Manual ElGamal.....	69
Gambar III.10 Activity Diagram Pembangkit Kunci Otomatis ElGamal	70
Gambar III.11 Activity Diagram Cek Prima.....	71
Gambar III.12 Activity Diagram Extended Euclidean	72
Gambar III.13 Activity Diagram Konversi ASCII ke Biner	73
Gambar III.14 Activity Diagram Konversi Biner ke Decimal.....	74
Gambar III.15 Activity Diagram Konversi Decimal ke Biner.....	75
Gambar III.16 Activity Diagram Konversi ASCII ke Karakter Keyboard	75
Gambar III.17 Activity Diagram Enkripsi Pesan dan Gambar	76
Gambar III.18 Activity Diagram Dekripsi Pesan dan Gambar	77
Gambar III.19 Activity Diagram Save	78
Gambar III.20 Activity Diagram Load	79
Gambar III.21 User Interface Design Menu Utama	80
Gambar III.22 User Interface Design Menu Pemilihan Algoritma	81
Gambar III.23 User Interface Design Enkripsi Pesan Rabin.....	81
Gambar III.24 User Interface Design Enkripsi Gambar Rabin	82
Gambar III.25 User Interface Design Dekripsi Pesan Rabin.....	83
Gambar III.26 User Interface Design Dekripsi Gambar Rabin.....	84
Gambar III.27 User Interface Design Enkripsi Pesan ElGamal	85
Gambar III.28 User Interface Design Enkripsi Gambar ElGamal.....	86
Gambar III.29 User Interface Design Dekripsi Pesan ElGamal	87

Gambar III.30 User Interface Design Dekripsi Gambar ElGamal	88
Gambar III.31 User Interface Design Enkripsi Pesan McEliece.....	89
Gambar III.32 User Interface Design Enkripsi Gambar McEliece	90
Gambar III.33 User Interface Design Dekripsi Pesan McEliece	91
Gambar III.34 User Interface Design Dekripsi Gambar McEliece.....	92
Gambar III.35 User Interface Design Menu Perbandingan Efisiensi	93
Gambar III.36 Class Diagram Design	94
Gambar IV.1 Relasi antar Class (Main Class).....	103
Gambar IV.2 Class Diagram (ElGamal Subsystem).....	106
Gambar IV.3 Class Diagram (McEliece Subsystem).....	109
Gambar IV.4 Class Diagram (Rabin Subsystem)	112
Gambar IV.5 Diagram Top Down.....	119
Gambar IV.6 User Interface Menu Utama.....	122
Gambar IV.7 User Interface Menu Pemilihan Algoritma.....	123
Gambar IV.8 User Interface Enkripsi Pesan Rabin	123
Gambar IV.9 User Interface Enkripsi Gambar Rabin.....	124
Gambar IV.10 User Interface Dekripsi Pesan Rabin	125
Gambar IV.11 User Interface Dekripsi Gambar Rabin	126
Gambar IV.12 User Interface Enkripsi Pesan ElGamal	127
Gambar IV.13 User Interface Enkripsi Gambar ElGamal	128
Gambar IV.14 User Interface Dekripsi Pesan ElGamal.....	129
Gambar IV.15 User Interface Dekripsi Gambar ElGamal.....	130
Gambar IV.16 User Interface Enkripsi Pesan McEliece	131
Gambar IV.17 User Interface Enkripsi Gambar McEliece	132
Gambar IV.18 User Interface Dekripsi Pesan McEliece	133
Gambar IV.19 User Interface Dekripsi Pesan McEliece	134
Gambar IV.20 User Interface Menu Perbandingan Efisiensi.....	135

DAFTAR TABEL

Tabel I.1 Definisi, Akronim, dan Singkatan	3
Tabel I.2 Time Schedule	8
Tabel III.1 Algoritma Extended Euclidean dengan masukan $a=4864$ dan $b=3458$	36
Tabel III.2 Jumlah parity (m) dan matriks (n,k)	38
Tabel III.3 Jumlah parity (m) dan polynomials.....	39
Tabel III.4 Tabel Konversi Pesan ke ASCII	45
Tabel III.5 Tabel Proses Enkripsi	47
Tabel III.6 Notasi Use Case Memilih Teknik Rabin	62
Tabel III.7 Notasi Use Case Memilih Teknik McEliece	63
Tabel III.8 Notasi Use Case Memilih Teknik ElGamal	63
Tabel IV.1 Tabel Ulasan Realisasi Fungsionalitas	121
Tabel V.1 Test Case Enkripsi dan Dekripsi dengan Teknik Rabin.....	136
Tabel V.2 Test Case Enkripsi dan Dekripsi dengan Teknik McEliece	137
Tabel V.3 Test Case Enkripsi dan Dekripsi dengan Teknik ElGamal	138
Tabel V.4 Test Case Melihat Hasil Perbandingan Algoritma (Efeciency)	139
Tabel V.5 Test Black Box Enkripsi dan Dekripsi dengan Teknik Rabin	140
Tabel V.6 Test Black Box Enkripsi dan Dekripsi dengan Teknik McEliece	143
Tabel V.7 Test Black Box Enkripsi dan Dekripsi dengan Teknik ElGamal.....	145
Tabel V.8 Test Black Box Melihat Hasil Perbandingan Algoritma (Efeciency)	147
Tabel V.9 Test White Box Enkripsi dan Dekripsi dengan Teknik Rabin.....	148
Tabel V.10 Test White Box Enkripsi dan Dekripsi dengan Teknik McEliece.....	149
Tabel V.11 Test White Box Enkripsi dan Dekripsi dengan Teknik ElGamal	150
Tabel V.12 Test White Box Melihat Hasil Perbandingan Algoritma (Efeciency).....	151

DAFTAR CUPLIKAN KODE PROGRAM

Program IV.1 Main Form	104
Program IV.2 Bangkit Kunci Otomatis ElGamal(Pesan)	107
Program IV.3 Enkripsi Pesan ElGamal	107
Program IV.4 Dekripsi Pesan ElGamal	107
Program IV.5 Bangkit Kunci Otomatis ElGamal(Gambar)	108
Program IV.6 Enkripsi Gambar ElGamal.....	108
Program IV.7 Dekripsi Gambar ElGamal	109
Program IV.8 Bangkit Kunci Otomatis McEliece(Pesan)	110
Program IV.9 Enkripsi Pesan McEliece	110
Program IV.10 Dekripsi Pesan McEliece	110
Program IV.11 Bangkit Kunci Otomatis McEliece (Gambar)	111
Program IV.12 Enkripsi Gambar McEliece	111
Program IV.13 Dekripsi Gambar McEliece	112
Program IV.14 Bangkit Kunci Otomatis Rabin(Pesan)	113
Program IV.15 Enkripsi Pesan Rabin.....	113
Program IV.16 Dekripsi Pesan Rabin	113
Program IV.17 Bangkit Kunci Otomatis Rabin (Gambar)	114
Program IV.18 Enkripsi Gambar Rabin.....	114
Program IV.19 Dekripsi Gambar Rabin.....	115
Program IV.20 Menggambar Diagram Batang	116
Program IV.21 Method-Method pada Class GEN_CHECK_PRIME	116
Program IV.22 Method-Method pada Class POWER_MOD.....	116
Program IV.23 Method-Method pada Class Image_Converter.....	117
Program IV.24 Method-Method pada Class MATRIKS_GEN.....	118
Program IV.25 Method Pencarian Error pada Hamming Code.....	118
Program IV.26 Method-Method pada Class EXTENDED_EUCLIDEAN.....	118

DAFTAR LAMPIRAN

LAMPIRAN A HASIL UJI COBA ENKRIPSI TEKNIK RABIN NO.1	A.1
LAMPIRAN A HASIL UJI COBA ENKRIPSI TEKNIK ELGAMAL NO.1	B.1
LAMPIRAN A HASIL UJI COBA ENKRIPSI TEKNIK MCELIECE NO.1	C.1
LAMPIRAN A HASIL PERBANDINGAN TIAP TEKNIK DALAM HAL UKURAN / SIZE	D.1
LAMPIRAN A HASIL PERBANDINGAN TIAP TEKNIK DALAM HAL JUMLAH KARAKTER	D.2
LAMPIRAN A HASIL PERBANDINGAN TIAP TEKNIK DALAM HAL KECEPATAN	D.3