

## DAFTAR ISI

SKRIPSI .....	i
PERSETUJUAN TUGAS AKHIR.....	ii
PENGESAHAN DEWAN PENGUJI.....	iii
PERNYATAAN KEASLIAN TUGAS AKHIR.....	iv
PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS .....	v
UCAPAN TERIMAKASIH.....	vi
ABSTRAK.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR .....	xi
DAFTAR TABEL.....	xiv
DAFTAR LAMPIRAN .....	xvi
BAB I.....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
BAB II.....	6
2.1 Tinjauan Studi .....	6
2.1.1 Aspek Ancaman Keamanan.....	10

2.1.2	Aspek Keamanan.....	11
2.1.3	Definisi dan Terminologi Kriptografi.....	12
2.1.4	<i>One-Time Pad</i> dan <i>Cipher Aliran (Stream Cipher)</i> .....	19
2.1.5	Algoritma yang Aman.....	24
2.1.6	Algoritma Blum Blum Shub.....	26
2.2	Kerangka Pemikiran.....	49
<b>BAB III</b> .....		50
3.1	Jenis Penelitian.....	50
3.2	Instrumen Penelitian.....	50
3.2.1	Kebutuhan Perangkat Lunak.....	50
3.2.2	Kebutuhan Perangkat Keras.....	51
3.3	Prosedur Pengumpulan Data.....	51
3.4	Teknik Analisa Data.....	52
3.5	Metode yang Diusulkan.....	52
3.5.1	Prosedur Enkripsi Data yang Diusulkan.....	52
3.5.2	Prosedur Dekripsi Data yang Diusulkan.....	54
3.6	Desain Tampilan Program.....	55
3.7	Eksperimen dan Cara Pengujian Metode.....	56
<b>BAB IV</b> .....		57
4.1	Desain Program.....	57
4.1.1	Desain Enkripsi dan Dekripsi Algoritma One Time Pad.....	57
4.1.2	Desain Pembangkit Kunci Blum Blum Shub.....	62
4.1.3	Desain Variasi Kunci.....	65
4.2	Tampilan Program One Time Pad dan Variasi Kunci Blum Blum Shub.....	78
4.3	Tampilan Pesan Peringatan Nilai Awal P, Q, dan S pada Program.....	83

4.4	Hasil Eksperimen One Time Pad dan Variasi Kunci Blum Blum Shub	87
4.4.1	Enkripsi BBS dengan <i>Least Significant Bit</i> dan $j$ buah bit	87
4.4.2	Enkripsi BBS dengan <i>LSB</i> , $j$ buah bit, dan iterasi	99
4.4.3	Enkripsi BBS dengan <i>LSB</i> , $j$ buah bit, dan <i>wrapping</i>	106
4.4.4	Enkripsi BBS dengan <i>LSB</i> , $j$ buah bit, iterasi dan <i>wrapping</i>	114
4.4.5	Eksperimen untuk dekripsi	121
4.5	Penemuan dalam pemilihan nilai awal sebagai kunci algoritma Blum Blum Shub	125
4.6	Pengujian	133
BAB V		134
5.1	Kesimpulan	134
5.2	Saran	135
JADWAL PENYUSUNAN TUGAS AKHIR		136
DAFTAR PUSTAKA		137
LAMPIRAN		139

## DAFTAR GAMBAR

Gambar 1 : Contoh plainteks dan cipherteks.....	14
Gambar 2 : Skema enkripsi dan dekripsi.....	17
Gambar 3 : Hubungan antara kriptografi dan kriptanalisis.....	19
Gambar 4 : Konsep <i>cipher</i> aliran.....	20
Gambar 5 : <i>One Time Pad</i> .....	21
Gambar 6 : Kerangka pemikiran.....	49
Gambar 7 : Flowchart Metode Enkripsi.....	53
Gambar 8 : Flowchart Metode Dekripsi.....	54
Gambar 9 : Desain Tampilan Program.....	55
Gambar 10 : Flowchart program enkripsi pada aplikasi <i>One Time Pad</i> .....	58
Gambar 11 : Flowchart program dekripsi pada aplikasi <i>One Time Pad</i> .....	60
Gambar 12 : Flowchart Pembangkitan Kunci.....	63
Gambar 13 : Kunci awal iterasi.....	67
Gambar 14 : Kunci setelah iterasi.....	68
Gambar 15 : Kunci awal <i>wrapping</i> .....	68
Gambar 16 : Kunci setelah <i>wrapping</i> .....	69
Gambar 17 : Kunci awal sebelum kombinasi iterasi dan <i>wrapping</i> .....	70
Gambar 18 : Kunci setelah <i>wrapping</i> .....	70
Gambar 19 : Kunci <i>error</i> setelah iterasi.....	71
Gambar 20 : Kunci awal kombinasi iterasi dan <i>wrapping</i> .....	72
Gambar 21 : Kunci setelah iterasi.....	72
Gambar 22 : Kunci setelah <i>wrapping</i> .....	73
Gambar 23 : Flowchart VARIASI KUNCI pada proses enkripsi.....	74
Gambar 24 : Flowchart VARIASI KUNCI pada proses dekripsi.....	76
Gambar 25 : Tampilan awal aplikasi.....	79
Gambar 26 : Tampilan form pada program.....	79
Gambar 27 : Tampilan <i>list box</i> pada program.....	82

Gambar 28 : Peringatan P tidak memenuhi $3 \text{ Mod } 4$ .....	83
Gambar 29 : Peringatan Q tidak memenuhi $3 \text{ Mod } 4$ .....	84
Gambar 30 : Peringatan P bukan bilangan prima.....	85
Gambar 31 : Peringatan Q bukan bilangan prima.....	85
Gambar 32 : Peringatan S tidak boleh kurang dari 2.....	86
Gambar 33 : Peringatan S tidak boleh lebih dari nilai N.....	86
Gambar 34 : Peringatan S dan N tidak relatif prima.....	87
Gambar 35 : File Hari ini Hujan.....	96
Gambar 36 : Pilih j buah bit untuk enkripsi dengan j.....	97
Gambar 37 : Memilih teks untuk proses enkripsi.....	97
Gambar 38 : Memilih folder penyimpanan file teks yang sudah dienkripsi.....	98
Gambar 39 : Pesan aplikasi bahwa file teks berhasil dienkripsi.....	98
Gambar 40 : Hasil enkripsi dari file Hari ini Hujan dengan LSB.....	99
Gambar 41 : Hasil enkripsi dari file Hari ini Hujan dengan $j = 2$ .....	99
Gambar 42 : Memilih Iterasi Key lalu input nilai iterasi.....	105
Gambar 43 : Memilih Iterasi Key dan j buah bit lalu input nilai iterasi.....	106
Gambar 44 : Hasil enkripsi dengan LSB dan iterasi=6.....	106
Gambar 45 : Hasil enkripsi dengan $j=2$ dan iterasi=6.....	106
Gambar 46 : Memilih Wrap Key lalu input nilai <i>wrapping</i> .....	113
Gambar 47 : Memilih Wrap Key dan j buah bit lalu input nilai <i>wrapping</i> .....	113
Gambar 48 : Hasil enkripsi dengan LSB dan <i>wrapping</i> =3.....	113
Gambar 49 : Hasil enkripsi dengan $j=2$ dan <i>wrapping</i> =3.....	114
Gambar 50 : Memilih Iterasi Wrap Key lalu input masing-masing nilai.....	120
Gambar 51 : Memilih Iterasi, Wrap Key, dan j buah bit lalu input nilai.....	121
Gambar 52 : Hasil enkripsi dengan LSB berikut iterasi =6 dan <i>wrapping</i> =3.....	121
Gambar 53 : Hasil enkripsi dengan $j=2$ berikut iterasi =6 dan <i>wrapping</i> =3.....	121
Gambar 54 : Memilih teks untuk proses dekripsi.....	124
Gambar 55 : Memilih penyimpanan file teks yang sudah didekripsi.....	124
Gambar 56 : Pesan aplikasi bahwa file teks berhasil didekripsi.....	125
Gambar 57 : File teks yang sukses didekripsi.....	125
Gambar 58 : Perulangan Pada Pembangkit Kunci.....	126

Gambar 59 : Hasil nilai kunci berubah seiring nilai s.....	127
Gambar 60 : Enkripsi Huruf Kapital A kunci LSB $p = 19, q = 19, s = 9$ .....	128
Gambar 61 : Enkripsi Huruf Kapital A kunci LSB $p = 31, q = 31, s = 9$ .....	129
Gambar 62 : Enkripsi Huruf Kapital A kunci LSB $p = 43, q = 43, s = 9$ .....	130
Gambar 63 : Hasil kunci = 0 dengan $p = 7, q = 19, s = 31$ .....	131
Gambar 64 : Keacakan kunci tak terbentuk dengan $p=11, q=23, s=24$ .....	132

## DAFTAR TABEL

Tabel 1. <i>State of the art</i> .....	8
Tabel 2. Tabel bit acak $z_i$ .....	30
Tabel 3. Tabel Plainteks.....	32
Tabel 4. Tabel Kunci $K_1$ sampai $K_3$ .....	38
Tabel 5. Tabel Kunci $K_4$ sampai $K_6$ .....	39
Tabel 6. Tabel Kunci $K_7$ sampai $K_9$ .....	39
Tabel 7. Tabel Kunci $K_{10}$ sampai $K_{12}$ .....	40
Tabel 8. Tabel Kunci $K_{13}$ sampai $K_{14}$ .....	40
Tabel 9. Tabel Plainteks.....	41
Tabel 10. Penjelasan form aplikasi pada program.....	80
Tabel 11. Penjelasan <i>list box</i> pada program.....	82
Tabel 12. Tabel Plainteks.....	88
Tabel 13. Tabel Kunci $K_1$ sampai $K_3$ menggunakan LSB dan $j$ .....	91
Tabel 14. Tabel Kunci $K_4$ sampai $K_6$ menggunakan LSB dan $j$ .....	91
Tabel 15. Tabel Kunci $K_7$ sampai $K_9$ menggunakan LSB dan $j$ .....	92
Tabel 16. Tabel Kunci $K_{10}$ sampai $K_{12}$ menggunakan LSB dan $j$ .....	92
Tabel 17. Tabel Kunci $K_{13}$ sampai $K_{14}$ menggunakan LSB dan $j$ .....	93
Tabel 18. Tabel Kunci $K_1$ sampai $K_3$ dengan Iterasi = 6.....	100
Tabel 19. Tabel Kunci $K_4$ sampai $K_6$ dengan Iterasi = 6.....	100
Tabel 20. Tabel Kunci $K_7$ sampai $K_9$ dengan Iterasi = 6.....	101
Tabel 21. Tabel Kunci $K_{10}$ sampai $K_{12}$ dengan Iterasi = 6.....	101
Tabel 22. Tabel Kunci $K_{13}$ sampai $K_{14}$ .....	102
Tabel 23. Tabel Kunci $K_1$ sampai $K_3$ dengan <i>wrapping</i> = 3.....	107
Tabel 24. Tabel Kunci $K_4$ sampai $K_6$ dengan <i>wrapping</i> = 3.....	108
Tabel 25. Tabel Kunci $K_7$ sampai $K_9$ dengan <i>wrapping</i> = 3.....	108
Tabel 26. Tabel Kunci $K_{10}$ sampai $K_{12}$ dengan <i>wrapping</i> = 3.....	109
Tabel 27. Tabel Kunci $K_{13}$ sampai $K_{14}$ dengan <i>wrapping</i> = 3.....	109

Tabel 28. Tabel Kunci $K_1$ sampai $K_3$ dengan iterasi=6 dan <i>wrapping</i> =3.....	115
Tabel 29. Tabel Kunci $K_4$ sampai $K_6$ dengan iterasi=6 dan <i>wrapping</i> =3 .....	115
Tabel 30. Tabel Kunci $K_7$ sampai $K_9$ dengan iterasi=6 dan <i>wrapping</i> =3 .....	116
Tabel 31. Tabel Kunci $K_{10}$ sampai $K_{12}$ dengan iterasi=6 dan <i>wrapping</i> =3.....	116
Tabel 32. Tabel Kunci $K_{13}$ sampai $K_{14}$ dengan iterasi=6 dan <i>wrapping</i> =3.....	117



## DAFTAR LAMPIRAN

Lampiran 1. Perhitungan $x_i$ Dalam Mencari $z_i$ .....	140
Lampiran 2. Objek Seratus File Berformat (.txt).....	144