

DAFTAR ISI

LEMBAR PERSETUJUAN	i
LEMBAR PENGESAHAN	ii
PERNYATAAN KEASLIAN SKRIPSI	iii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	4
1.4 Tujuan dan Manfaat	4
1.5 Metodologi Penelitian	5
1.6 Sistematika Penulisan	6
BAB II LANDASAN TEORI	7
2.1 Kriptografi	7
2.1.1 Algoritma <i>Linear Block Cipher</i>	9
2.1.2 Algoritma Kunci Simetris	12

2.1 Matriks	15
2.2.1 Operasi Matriks	15
2.2.2 Determinan Matriks	18
2.2.3 Invers Matriks	20
2.2 Aritmatika Modulo	21
2.3.1 Operasi Aritmatika Modulo	23
2.3.2 Kongruensi Matriks	24
2.3.3 Invers Modulo	25
2.3 Algoritma <i>Euclidean</i> dan <i>Extended Euclidean</i>	25
2.4.1 Algoritma <i>Euclidean</i>	25
2.4.2 <i>Extended Euclidean</i>	27
2.4 <i>American Standard Code for Information Interchange (ASCII)</i>	29
BAB III MODIFIKASI ALGORITMA <i>LINEAR BLOCK CIPHER</i> DENGAN KUNCI SIMETRIS SEDERHANA	32
3.1 Membangkitkan Kunci Simetris	32
3.2 Proses Enkripsi	36
3.2.1 Penerapan Enkripsi Algoritma <i>Linear Block Cipher</i>	36
3.2.2 Penerapan Enkripsi Algoritma Kunci Simetris Sederhana	39
3.3 Proses Dekripsi	41
3.3.1 Penerapan Dekripsi Algoritma Kunci Simetris Sederhana	41
3.3.2 Penerapan Dekripsi Algoritma <i>Linear Block Cipher</i>	43
BAB IV IMPLEMENTASI DAN PENGUJIAN	48
4.1 Simulasi Pengiriman Pesan	48
4.2 Proses Enkripsi	52

4.2.1 Menentukan Matriks Kunci	52
4.2.2 Konversi <i>Plaintext</i> ke ASCII	52
4.2.3 Pembentukan Matriks <i>Plaintext</i>	53
4.2.4 Enkripsi Menggunakan Algoritma <i>Linear Block Cipher</i>	52
4.2.5 Menentukan Kunci Simetris dan Pembangkitan Kunci	53
4.2.6 Enkripsi Menggunakan Algoritma Kunci Simetris Sederhana	54
4.3 Proses Dekripsi	55
4.3.1 Menentukan Invers Kunci Simetris dan Pembangkitan <i>Round Key</i>	55
4.3.2 Dekripsi Menggunakan Algoritma Kunci Simetris Sederhana	56
4.3.3 Menentukan Invers Matriks Kunci <i>Linear Block Cipher</i>	57
4.3.1 Dekripsi Menggunakan Algoritma <i>Linear Block Cipher</i>	60
4.4 Penyusunan Kembali <i>Plaintext</i>	61
BAB V PENUTUP	64
5.1 Kesimpulan	64
5.2 Saran	65
DAFTAR PUSTAKA	66

DAFTAR GAMBAR

Gambar 3.1	Proses Membangkitkan Kunci Simetris	35
Gambar 3.2	Proses Enkripsi Algoritma <i>Linear Block Cipher</i> dengan Kunci Simetris Sederhana	46
Gambar 3.3	Proses Dekripsi Algoritma Kunci Simetris Sederhana dengan <i>Linear Block Cipher</i>	47
Gambar 4.1	Simulasi Pengiriman Pesan	50



DAFTAR TABEL

Tabel 2.1	Representasi ASCII	34
Tabel 4.1	Konversi <i>Plaintext</i> ke ASCII	51
Tabel 4.2	Pembangkitan <i>Round Key</i>	53
Tabel 4.3	Pembangkitan Invers <i>Round Key</i>	56
Tabel 4.4	Konversi <i>Plaintext</i> ke Karakter	62



DAFTAR LAMPIRAN

Lampiran A	Karakter ASCII 8 - bit	A - 1
-------------------	------------------------------	-------

