DAFTAR ISI

ABSTRAK……..……..……..……..……..……..……..…… i
ABSTRACT……..……..……..……..……..……..……..… ii
KATA PENGANTAR……..……..……..……..……..……..……. iii
DAFTAR ISI ……..……..……..……..……..……..……..…v
DAFTAR GAMBAR……..……..……..……..……..……..…… viii
DAFTAR TABEL……..……..……..……..……..……..… x
DAFTAR SIMBOL……..……..……..……..……..……..… xi

BAB I PENDAHULUAN

1.1 Latar Belakang……..……..……..……..……..……. 1
1.2 Identifikasi Masalah……..……..……..……..……. 2
1.3 Maksud dan Tujuan……..……..……..……..…….. 2
1.4 Batasan Masalah……..……..……..……..……..……. 3
1.5 Metodologi Penelitian……..……..……..……..……. 3
1.6 Sistematika Penulisan……..……..……..……..…… 5

BAB II LANDASAN TEORI

2.1 Kriptografi……..……..……..……..……..……. 6
2.2 Kriptografi dan Sistem Informasi……..……..……..……. 7
2.3 Mekanisme Kriptografi……..……..……..……..……. 8
2.4 Enkripsi dan Dekripsi……..……..……..……..……. 10
2.4.1 Enkripsi……..……..……..……..……..……. 10
2.4.2 Dekripsi……..……..……..……..……..……. 11
2.5 Algoritma Kriptografi……..……..……..……..……. 12
2.5.1 Kunci Simetris……..……..……..……..…… 12
2.5.2 Kunci Asimetris……..……..……..……..……. 16
2.6 Algoritma LOKI97……..……..……..……..…… 18
2.6.1 Spesifikasi LOKI97……..……..……..……..…….. 18
2.7 Teori Angka……..……..……..……..……..……. 20

2.7.1 Aritmatika Modular……. 20
2.7.2 Invers Modulo……. 20
2.7.3 Operasi Logika XOR……. 21
2.8 Borland C++ Builder 6……. 22

BAB III ANALISIS DAN PERANCANGAN

3.1 Analisis……. 24
3.1.1 Elemen pembangun LOKI97……. 24
3.1.1.1 Feistal Network……. 24
3.1.1.2 Data Computation……. 25
3.1.1.3 Penjadwalan Kunci……. 25
3.1.1.4 Fungsi f(A,B) ……. 25
3.1.1.5 S-Box……. 25
3.1.2 Spesifikasi Proses……. 26
3.1.2.1 Algoritma Enkripsi……. 26
3.1.2.2 Algoritma Dekripsi……. 31
3.1.3 Analisis Umum Sistem……. 33
3.1.4 Kebutuhan Fungsional……. 33
3.1.5 Algoritma Pembanding……. 34
3.1.5.1 Blowfish……. 34
3.1.5.2 DES……. 37
3.1.5.3 IDEA……. 38
3.2 Perancangan……. 42
3.2.1 Diagram Konteks……. 42
3.2.2 DFD Level 1……. 43
3.2.3 DFD Level 2……. 44
3.2.4 Perancangan Antar Muka……. 47

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi……52

4.1.1 Tampilan Program…… 52

4.1.2 Spesifikasi Sistem…….56

4.1.2.1 Spesifikasi perangkat keras…….56

4.1.2.2 Spesifikasi Perangkat Lunak…… 57

4.2 Pengujian Sistem……. 57

4.2.1 Pengujian Fungsional……57

4.2.2 Kesimpulan Pengujian…… 60

4.2.3 Pengujian Aplikasi Menggunakan Data Real…… 60

4.2.4 Pengujian Algoritma LOKI97……61

4.2.5 Pengujian Algoritma Pembanding (Blowfish) ……64

4.2.6 Perbandingan Algoritma LOKI97 (panjang kunci 128)

dan Blowfish…… 65

4.2.7 Simulasi Panjang kuci LOKI97…… 69

4.3 Hasil Pengujian dan Analisa……70

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan…… 72

5.2 Saran…… 73

DAFTAR PUSTAKA

LAMPIRAN