DAFTAR ISI

LEMBAR JUDUL

LEMBAR PENGESAHAN

ABSTRAK i

ABSTRACT ii

LEMBAR PERSEMBAHAN iii

KATA PENGANTAR iv

DAFTAR ISI v

DAFTAR TABEL ix

DAFTAR GAMBAR xi

DAFTAR SINGKATAN DAN SIMBOL xvi

DAFTAR LAMPIRAN xvii

BAB I PENDAHULUAN 1

1.1 Latar Belakang Masalah 1

1.2 Identifikasi Masalah 4

1.3 Maksud dan Tujuan 5

1.4 Batasan Masalah 5

1.5 Metodologi Penelitian 6

1.6 Sistematika Penulisan 8

BAB II TINJAUAN PUSTAKA 9

2.1 Kriptografi 9

2.1.1 Pengertian Kriptografi 9

2.1.2 Tujuan Kriptografi 9

2.1.3 Jenis Algoritma Kriptografi 10
2.1.3.1 Kriptografi Simetri (*Symetric Cryptography*) 10
2.1.3.2 Kriptografi Asimetri (*Asymetric Cryptography*) 11
2.1.4 Tinjauan Matematis 12
2.1.4.1 Konsep Dasar Kriptografi 12
2.1.4.2 Aritmatika Modular 13
2.1.5 Cipher Blok 14
2.1.6 *Avalanche Effect* 16
2.1.7 Proses Padding 16
2.2 Algoritma Kriptografi *Vertical Bit Rotation* (VBR) 17
2.2.1 Pembentukan Blok 17
2.2.2 Proses Enkripsi 18
2.2.3 Proses Dekripsi 20
BAB III ANALISIS DAN PERANCANGAN SISTEM 21
3.1 Analisis Masalah 21
3.2 Analisis Algoritma Kriptogafi VBR 22
3.2.1 Prosedural Enkripsi Dan Dekripsi Algoritma Kriptografi VBR ... 22
3.2.2 Analisis Blok Penyandian pada Algoritma Kriptografi VBR 23
3.2.3 Analisis Rotasi Bit pada Algoritma Kriptografi VBR 25
3.2.4 Analisis Kunci (*K*) dan Variabel Rotasi (*r*) 26
3.2.5 Tidak Ada Perubahan Bit pada Algoritma Kriptografi VBR 27
3.2.6 *Avalanche Effect* pada Algoritma Kriptografi VBR 27
3.3 Modifikasi pada Algoritma Kriptogafi VBR 29
3.3.1 Modifikasi Ukuran Tabel Bit 29

3.3.2 Penambahan *SubBlok* dan Proses *Padding* 30
3.3.3 Aturan Tambahan Variabel Rotasi (r) 32
3.3.4 Proses Modulo Variabel Rotasi 32
3.3.5 Proses Initial Rotation dan Proses Final Rotation 33
3.3.6 Modifikasi Kunci (K) 33
3.3.7 Ekspansi Kunci (K), Proses Add Key, dan Proses Add SubKey .. 34
3.3.8 Proses SubBlock Rotation 35
3.3.9 Proses Byte Substitution 36
3.3.10 Proses Binary Rotation dan Proses Inverse Binary Rotation 37
3.3.11 Putaran (Round) pada Algoritma Kriptograf VBR 32 Bit 38
3.3.12 Prosedural Enkripsi dan Dekripsi Algoritma Kriptografi VBR 32 Bit 38
3.3.12 Mirrored Key Generation (MKG) 39
3.4 Analisis Pengguna 40
3.5 Analisis Perangkat Lunak 41
3.6 Analisis Perangkat Keras 42
3.7 Gambaran Umum Sistem 42
3.8 Perancangan Sistem 43
3.8.1 Perancangan Model Sistem 43
3.8.1.1 *Entity Relationship Diagram* 43
3.8.1.2 *Data Flow Diagram* 44
3.8.1.3 Kamus Data 48
3.8.1.4 Spesifikasi Proses 54
3.8.1.5 Skema Relasi 59

3.8.1.6 Struktur Data 60
3.8.2 Perancangan Menu 61
3.8.3 Perancangan Antarmuka (*Interface*) 62
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM 82
4.1 Implementasi 82
4.1.1 Perangkat Lunak Pendukung 82
4.1.2 Perangkat Keras 83
4.1.3 Implementasi Database 84
4.1.4 Implementasi Pengguna 84
4.1.5 Implementasi Data 85
4.1.6 Implementasi Antarmuka 85
4.2 Pengujian Sistem 93
4.2.1 Pengujian Terhadap Masukan 93
4.2.2 Pengujian Keamanan Berdasarkan *Avalanche Effect* 95
4.2.2.1 Pengujian dengan Kunci Berbeda 1 Bit 97
4.2.2.1 Pengujian dengan Plainteks Berbeda 1 Bit 97
4.2.3 Pengujian Pada Sistem Operasi 32 Bit dan Sistem Operasi 64 Bit . 98
4.3 Analisa Data Eksperimen (*Nilai Avalanche Effect*) 99
4.4 Analisa Modifikasi Algoritma Kriptografi VBR 32 Bit 101
BAB V KESIMPULAN DAN SARAN 103
5.1 Kesimpulan 103
5.2 Saran 104
DAFTAR PUSTAKA