DAFTAR ISI

LEMBAR PENGESAHAN NASKAH SKRIPSI iii
PEDOMAN PENGGUNAAN SKRIPSI iv
SURAT PERNYAATAAN TENTANG ORSINALITAS v
KATA PENGANTAR vi
ABSTRAK viii
ABSTRACT ix
DAFTAR ISI x
DAFTAR TABEL xiii
DAFTAR GAMBAR xiv
BAB I PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Rumusan Masalah 2
1.3. Tujuan 2
1.4. Manfaat 3
1.5. Batasan Masalah 3
BAB II TINJAUAN PUSTAKA 4
2.1. Kriptografi 4
2.1.1 Definisi Kripografi 4
2.1.2 Kriptografi Modern 5
2.1.3 Operasi Aljabar 6
2.1.3.1 Field GF(2^8) 6
2.2. Algoritma *Advanced Encryption Standard* (AES) 7
2.2.1 Enkripsi *Advanced Encryption Standard* (AES) 8
2.2.2 Deskripsi *Advanced Encryption Standard* (AES) 12
2.2.3 Ekspansi Kunci *Advanced Encryption Standard* (AES) 16
2.3. File MP3 18
2.4. Microsoft Visual Basic 6.0 19

2.5. Binary Viewer 19
BAB III METODOLOGI PENELITIAN 20
BAB IV PEMBAHASAN 26
4.1 Enkripsi File MP3 Menggunakan Algoritma *Advanced Encryption Standard* (AES) 26
4.1.1 Mengkonversi File MP3 ke *Bytes* 26
4.1.2 Ekspansi Kunci Algoritma *Advanced Encryption Standard* (AES) 27
4.1.2.1 Proses *Rotword (Rotate)* 28
4.1.2.2 Proses *SubBytes* 29
4.1.2.3 Operasi RCon dan Operasi XOR dengan w[i-1] Kunci Ronde Sebelumnya 32
4.1.3 Mengenkripsi Bytes dari File menggunakan Algoritma *Advanced Encryption Standard* (AES) 32
4.1.3.1 Proses *AddRoundKey* 34
4.1.3.2 Proses *SubBytes* 34
4.1.3.3 Proses *ShiftRow* 35
4.1.3.4 Proses *MixColoumns* 36
4.1.4 Menyusun Bytes untuk Output File MP3 36
4.2 Deskripsi File MP3 Menggunakan Algoritma *Advanced Encryption Standard* (AES) 37
4.2.1 Mengkonversi File MP3 ke *Bytes* 38
4.2.2 Ekspansi Kunci Algoritma *Advanced Encryption Standard* (AES) 38
4.2.3 Mendeskripsi Bytes dari File Menggunakan Algoritma *Advanced Encryption Standard* (AES) 38
4.2.3.1 Proses *AddRoundKey* 39
4.2.3.2 Proses *InvSubBytes* 40
4.2.3.3 Proses *InvShiftRow* 41
4.2.3.4 Proses *InvMixColoumns* 42
4.2.4 Menyusun Bytes untuk Output File MP3 43

4.3 Penyelesaian Secara Manual Enkripsi Menggunakan Algoritma *Advanced Encryption Standard* (AES).....43
4.3.1 Mengambil Nilai *Byte* pada File MP3.....43
4.3.2 Membangkitkan Kunci (Ekspansi Kunci).....44
4.3.3 Mengenkripsi Bilangan Hexadesimal dengan Algoritma *Advanced Encryption Standard* (AES).....50
4.4 Penyelesaian Secara Manual Deskripsi Menggunakan Algoritma *Advanced Encryption Standard* (AES).....54
4.4.1 Mengambil Nilai *Byte* pada File MP3.....54
4.4.2 Membangkitkan Kunci (Ekspansi Kunci).....55
4.4.3 Mengdeskripsi Bilangan Hexadesimal dengan Algoritma *Advanced Encryption Standard* (AES).....57
4.5 Implementasi Program Enkripsi dan Deskripsi pada File MP3 menggunakan Algoritma *Advanced Encryption Standard* (AES).....61
BAB V PENUTUP.....65
5.1 Kesimpulan.....65
5.2 Saran.....66
DAFTAR PUSTAKA.....67

DAFTAR TABEL

Tabel	Judul	Halaman
2.1	Jumlah Putaran berdasarkan panjang kunci	8
2.2	Tabel RCon	17

DAFTAR GAMBAR

Tabel	Judul	Halaman
2.1	Proses AddRoundKey	7
2.2	Proses SubBytes	8
2.3	Proses ShiftRows	9
2.4	Proses AddRoundKey	11
2.5	Tabel InvS-Box	12
2.6	Proses InvShiftRows	13
2.7	Proses *Rotate (RotWord)*	15
3.1	Flowchart enkripsi AES	21
3.2	Flowchart deskripsi AES	22
3.3	Flowchart Ekspansi kunci AES	23
4.1	Prosedur Proses Enkripsi	26
4.2	Prosedur mengkonversi file MP3 ke *Bytes*	27
4.3	Prosedur Ekspans KunciAlgoritma *Advanced Encryption Standard* (AES)	28
4.4	Prosedur *RotWord*	28
4.5	Prosedur *SubBytes pada* Kunci	29
4.6	Prosedur Membuat Tabel S-Box	29
4.7	Prosedur Operasi *SubBytes*	30
4.8	Prosedur Invers Multiplikatif	30
4.9	Prosedur Perputaran Bit	31
4.10	Prosedur Operasi Perkalian Galios Field	31
4.11	Prosedur RCon dan Operasi XOR dengan w[i-1] Kunci Ronde Sebelumnya	32
4.12	Prosedur Ekripsi *Bytes*	33
4.13	Prosedur *AddRoundKey*	34

4.14	Prosedur *SubBytes*	35
4.15	Prosedur *ShiftRow*	35
4.16	Prosedur*MixColoumns*	36
4.17	Prosedur Menyusun *Bytes*	37
4.18	Prosedur Proses Deskripsi	38
4.19	Prosedur Deskripsi *Bytes*	39
4.20	Prosedur *InvSubBytes*	40
4.21	Prosedur Membuat Tabel InvS-Box	41
4.22	Prosedur Operasi *InvSubBytes*	41
4.23	Prosedur *InvShiftRow*	42
4.24	Prosedur *InvMixColoumns*	43
4.25	Bytes Manual Sebelum Dienkripsi	44
4.26	Mengubah Barisan Bytes Sebelum Dienkripsi menjadi Matriks	50
4.27	Bytes Manual Sebelum Dideskripsi	55
4.28	Mengubah Barisan Bytes Sebelum Dideskripsi menjadi Matriks	57
4.29	Bytes Sebelum Dienkripsi	62
4.30	Bytes Setelah Dienkripsi	63
4.31	Bytes Setelah Dideskripsi	64