

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL	viii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Kerangka Pemikiran	4
1.6 Sistematika Penulisan	4
BAB II KAJIAN LITERATUR	6
2.1 Tinjauan Pustaka	6
2.1.1 The State of The Art	6
2.2 Landasan Teori	8
2.2.1 Pengertian Kriptografi	8
2.2.2 Pengertian Kompresi	11
2.2.3 Advanced Encryption Standards (AES)	11
2.2.4 Struktur Proses Enkripsi AES 128 bit	12
2.2.5 Struktur Proses Dekripsi AES 128 bit	13
2.2.6 Transformasi – transformasi algoritma AES	13
2.2.7 Rumus Akurasi Algoritma	18
2.3 Algoritma Lempel-ziv-Welch (LZW)	19
2.4 Model Prototyping	19
2.5 Aplikasi Pendukung	21
2.5.1 Pemrograman PHP	21
2.5.2 MySQL	21
2.5.3 Laravel Framework	22
2.5.4 UML	22
2.5.5 Use Case Diagram	23
2.5.6 Activity Diagram	24
BAB III METODOLOGI PENELITIAN	25
3.1 Analisis Sistem	25
3.2 Analisis Masalah	25
3.3 Analisis Kebutuhan	25
3.3.1 Pemodelan Kebutuhan Sistem	25
3.3.2 Kebutuhan Perangkat Keras (Hardware)	25
3.3.3 Kebutuhan Perangkat Lunak (Software)	26
3.3.4 Pengguna (Brainware)	26
3.3.5 Analisis Algoritma AES (Advanced Encryption Standard)	26
3.3.6 Analisis Algoritma LZW (Lempel-Ziv-Welch)	34
3.4 Desain Sistem	36
3.4.1 Use Case Diagram	36
3.4.2 Definisi Aktor	37
3.4.3 Definisi Use Case	37

3.4.4	Skenario Use Case	38
3.4.5	Perancangan Activity Diagram	40
3.4.6	Perancangan <i>Class Diagram</i>	45
3.4.7	Perancangan <i>Sequence Diagram</i>	46
3.5	Prototype Sistem	49
3.5.1	Arsitektur Sistem Usulan	49
3.5.2	Perancangan User Interface	50
BAB IV HASIL DAN PEMBAHASAN		55
4.1	Implementasi	55
4.1.1	Implementasi Perangkat Keras	55
4.1.2	Implementasi Perangkat Lunak	55
4.1.3	Implementasi User Interfaces	56
4.1.4	Implementasi Algoritma AES dan LZW	61
4.2	Pengujian	68
4.2.1	Pengujian <i>Black box</i>	68
4.2.2	Pengujian Algoritma	68
4.2.3	Rencana Pengujian	74
BAB V SIMPULAN DAN SARAN		79
5.1	Kesimpulan	79
5.2	Saran	79
DAFTAR PUSTAKA		80



DAFTAR GAMBAR

Gambar 1.1 Kerangka Pemikiran	4
Gambar 2.1 Skema proses Kriptografi [13]	10
Gambar 2.2 Skema Dekripsi AES [13]	13
Gambar 2.3 Tabel substitusi S-Box [13]	14
Gambar 2.4 Proses ShiftRows [13]	15
Gambar 2.5 Tabel inverse S-Box [13]	17
Gambar 2.6 Ilustrasi Transformasi InvShiftRows [13]	18
Gambar 2.7 Ilustrasi Persamaan [13]	18
Gambar 2.8 Life Cycle [18]	20
Gambar 3.1 Flowchart proses kompresi [29]	35
Gambar 3.2 Tahapan kompresi LZW [29]	36
Gambar 3.3 Use Case Diagram Sistem	37
Gambar 3.4 Aktivitas autentikasi dan authorisasi user	41
Gambar 3.5 Aktivitas Upload File	42
Gambar 3.6 Diagram aktivitas Registrasi	43
Gambar 3.7 Diagram Aktivitas view data, download, dan hapus data	44
Gambar 3.8 Activity Diagram Upload Data file	45
Gambar 3.9 Class Diagram	46
Gambar 3.10 Sequence Diagram Registration	47
Gambar 3.11 Sequence Diagram File Management	48
Gambar 3.12 Sequence Diagram AES Encryption dan LZW Compression	49
Gambar 3.13 Arsitektur Sistem Pengamanan File	50
Gambar 3.14 Perancangan UI Login	51
Gambar 3.15 Perancangan UI Registrasi	51
Gambar 3.16 Perancangan UI List File	52
Gambar 3.17 Perancangan UI Upload File	52
Gambar 4.1 Halaman Login	56
Gambar 4.2 Halaman Registrasi	57
Gambar 4.3 Halaman File Storage	58
Gambar 4.4 Input Password untuk download file	58
Gambar 4.5 Proses Hapus Data	59
Gambar 4.6 Halaman Upload File	59
Gambar 4.7 Hasil upload file di Amazon S3	60
Gambar 4.8 Notifikasi Sistem Error	60
Gambar 4.9 Performa Enkripsi dan Dekripsi	70
Gambar 4.10 Waktu enkripsi dan dekripsi	71
Gambar 4.11 Performa Kompresi dan Dekompresi	73
Gambar 4.12 Waktu kompresi dan dekompresi	74

DAFTAR TABEL

Tabel 2.1 State of The Art	7
Tabel 2.2 State of The Art (lanjutan)	8
Tabel 2.3 Hubungan Panjang key AES dan jumlah round key	12
Tabel 2.4 Use Case	23
Tabel 2.5 Activity Diagram [26]	24
Rumus 2.1 Persamaan 1	16
Rumus 2.2 Persamaan 2	16
Rumus 2.3 Persamaan 3	16
Rumus 2.4 Rumus Akurasi	18
Tabel 3.1 Input plaintext dan key kedalam matriks	27
Tabel 3.2 Ubah plaintext dan key state 0 menjadi hexadesimal	27
Tabel 3.3 Operasi XOR antara plaintext dengan key state 0	27
Tabel 3.4 S-Box	28
Tabel 3.5 Hasil substitusi key dengan tabel S-Box	28
Tabel 3.6 RCON table atau key schedule	28
Tabel 3.7 RotWord dan Sub-Byte column terakhir Key State 0	29
Tabel 3.8 Perhitungan Key State 0 Row 1	29
Tabel 3.9 Perhitungan Key State 0 Column 2 dan 3	29
Tabel 3.10 Perhitungan Key State 0 Column 4 dan hasil Key Sate 1	30
Tabel 3.11 Proses hasil addRoundKey subBytes	30
Tabel 3.12 Pergeseran baris pertama	30
Tabel 3.13 Pergeseran baris kedua	31
Tabel 3.14 Pergeseran baris ketiga	31
Tabel 3.15 Pergeseran baris keempat	31
Tabel 3.16 Polynomial	32
Tabel 3.17 Hasil Mix Column	33
Tabel 3.18 Operasi XOR Hasil Mix Column dengan Round Key 1	34
Tabel 3.19 Definisi Aktor Use Case	37
Tabel 3.20 Definisi Use Case	37
Tabel 3.21 Skenario Use Case Registration	38
Tabel 3.22 File Management	38
Tabel 3.23 Download File	39
Tabel 3.24 Delete File	39
Tabel 3.25 Skenario Use Case Upload File	40
Tabel 3.26 Skenario Use AES Encryption and LZW Compression	40
Tabel 4.1 Spesifikasi Perangkat Keras Implementasi Sistem	55

Tabel 4.2 Spesifikasi Perangkat Lunak Implementasi Sistem	55
Tabel 4.3 Table Test Ccase Equivalent Class Partitioning	69
Tabel 4.4 Table Test Case Equivalent Class Partitioning	72
Tabel 4.5 Rencana Pengujian Sistem	74
Tabel 4.6 Pengujian Fungsionalitas	75
Tabel 4.7 Pengujian Fungsionalitas (Lanjutan)	76
Tabel 4.8 Pengujian Fungsionalitas (Lanjutan)	77
Rumus 4. 1 Perhitungan Akurasi Algoritma AES	70
Rumus 4. 2 Perhitungan Akurasi Algoritma LZW	73

