

IMPLEMENTASI KEAMANAN DOKUMEN RAHASIA DESA MANGGIS MENGGUNAKAN METODE AES

ABSTRAK

Keamanan data saat ini menjadi fokus utama di era digitalisasi, karena pengaruh kemajuan teknologi yang sangat pesat celah keamanan dapat dimanfaatkan oleh pihak yang tidak bermoral maupun tidak bertanggung jawab. Kriptografi adalah ilmu yang mengkaji Teknik pengacakan data dan enkripsi adalah salah satu cara untuk mengamankan data agar tetap aman dan terjaga kerahasiaannya. Banyak instansi pemerintah berupaya meningkatkan sistem keamanan tersebut, namun masih banyak instansi pemerintah yang melakukan pengamanan data dengan cara manual. Tetapi pengamanan data dengan cara manual sangat memiliki banyak kekhawatiran dan resiko yang tinggi akan terjadinya kebocoran data atau pencurian data pada pemerintahan. *Advanced Encryption Standard* (AES) adalah salah satu algoritma kriptografi yang sering kali digunakan untuk pengamanan data pada Perusahaan, instansi, maupun data pribadi dan *Advanced Encryption Standard* (AES) merupakan standar enkripsi yang sangat aman dan sulit untuk ditembus. Dengan menggunakan AES, dokumen yang berisi informasi penting dan sensitif dapat dienkripsi sehingga tidak dapat dibaca oleh pihak yang tidak bertanggungjawab. Oleh karena itu, peneliti memilih AES sebagai metode pengamanan dokumen yang dirasa sangat aman dan sulit sekali untuk ditembus celah keamanannya.

Kata Kunci : AES, Enkripsi, Dekripsi, Keamanan Dokumen

DAFTAR ISI

ABSTRAK.....	iv
KATA PENGANTAR	v
DAFTAR ISI	viii
DAFTAR TABEL	x
DAFTAR GAMBAR.....	xi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Peneliti	5
1.5 Manfaat Penelitian.....	5
BAB II TINJAUAN PUSTAKA.....	6
2.1 Studi Literatur	6
2.2 Landasan Teori.....	11
2.2.1 Keamanan Data.....	11
2.2.2 Kriptografi Advanced Encryption Standard (AES)	12
2.2.3 Proses Enkripsi Algoritma <i>Advanced Enryption Standard</i> (AES)	14
2.2.4 Proses Dekripsi Algoritma <i>Advanced Enryption Standard</i> (AES)	15
BAB III METODOLOGI PENELITIAN	17
3.1 Metode Penelitian	17
3.2 Alur Penelitian	18
3.2.1 Analisa Kebutuhan Sistem	20
3.2.2 Rancangan Analisa Sistem	21
3.2.3 Desain Sistem Aplikasi	22
3.2.4 Rancangan Desain Aplikasi (<i>Wireframe</i>).....	24
BAB IV IMPLEMENTASI.....	34
4.1 Spesifikasi Kebutuhan.....	34

4.1.1 Alat dan Bahan.....	34
4.2 Implementasi Hasil.....	35
4.2.1 Tampilan Halaman Login	35
4.2.2 Tampilan Beranda (<i>Dashboard</i>)	36
4.2.3 Tampilan Menu Encrypt.....	36
4.2.4 Tampilan Menu Decrypt	38
4.2.5 Tampilan Menu List File.....	39
4.2.6 Tampilan Menu Help	40
4.2.7 Tampilan Menu About	40
4.3 Tampilan Berkas Setelah Enkripsi dan Dekripsi	41
4.4 Pengujian <i>Avalanche Effect</i> (AE)	43
4.5 Pengujian Kecepatan Proses Enkripsi dan Dekripsi	45
4.6 Pengujian Sistem Aplikasi	46
4.7 Perbandingan Aplikasi	49
BAB V PENUTUP	52
5.1 Kesimpulan.....	52
5.2 Saran	53
RIWAYAT HIDUP	53
LAMPIRAN I	54
LAMPIRAN II.....	55

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu	10
Tabel 2.2 Perbandingan Jumlah Round dan Key	14
Tabel 4.1 Pengujian Avalanche Effect.....	44
Tabel 4.2 Pengujian Rasio Kecepatan	45
Tabel 4.3 Tabel Pengujian Blackbox	47
Tabel 4.4 Tabel Perbandingan Aplikasi.....	49

DAFTAR GAMBAR

Gambar 2.1	Proses Algoritma Enkripsi Metode AES	15
Gambar 2.2	Proses Algoritma Dekripsi Metode AES	16
Gambar 3.1	Metode SDLC.....	17
Gambar 3.2	Alur Penelitian	19
Gambar 3.3	Rancangan Alur Sistem Aplikasi.....	22
Gambar 3.4	Desain Sistem Enkripsi	23
Gambar 3.5	Desain Sistem Dekripsi.....	24
Gambar 3.6	Tampilan Halaman Login	25
Gambar 3.7	Tampilan Beranda (Dashboard)	26
Gambar 3.8	Tampilan Proses Encrypt	27
Gambar 3.9	Tampilan Proses Decrypt	28
Gambar 3.10	Tampilan Menu List file yang Telah Dienkripsi	30
Gambar 3.11	Tampilan Menu Help.....	31
Gambar 3.12	Tampilan Menu About	32
Gambar 4.1	Tampilan Halaman Login	35
Gambar 4.2	Tampilan Beranda (Dashboard)	36
Gambar 4.3	Tampilan Menu Encrypt	37
Gambar 4.4	Tampilan Proses Hasil Encrypt	37
Gambar 4.5	Tampilan Menu Decrypt	38
Gambar 4.6	Tampilan Proses Hasil Decrypt	39
Gambar 4.7	Tampilan Menu List File	39
Gambar 4.8	Tampilan Menu Help.....	40
Gambar 4.9	Tampilan Menu About	41
Gambar 4.10	Dokumen PDF Sebelum Dienkripsi.....	42
Gambar 4.11	Dokumen PDF Sesudah Dienkripsi	43