

IMPLEMENTASI KEAMANAN FORMULIR DATA SISWA PADA WEB PENDAFTARAN DENGAN METODE AES

ABSTRAK

Perkembangan teknologi digital yang pesat membawa manfaat besar bagi kehidupan sehari-hari, namun juga menimbulkan tantangan baru terkait keamanan data. Keamanan data menjadi semakin krusial, terutama dalam lingkungan pendidikan, di mana perlindungan data siswa sangat penting untuk mencegah penyalahgunaan oleh pihak yang tidak bertanggung jawab. SPS Tapos, sebagai lembaga pendidikan, menghadapi tantangan ini dalam mengelola formulir pendaftaran siswa yang mengandung informasi pribadi sensitif. Saat ini, proses pendaftaran masih dilakukan secara manual, yang rentan terhadap risiko keamanan. Untuk mengatasi permasalahan tersebut, diperlukan sistem pendaftaran berbasis web yang dapat mengamankan data siswa melalui metode enkripsi. Penelitian ini mengusulkan penerapan Advanced Encryption Standard (AES) sebagai solusi untuk melindungi data siswa. AES merupakan algoritma kriptografi yang kuat dan efisien, dengan kemampuan enkripsi dan dekripsi yang menggunakan kunci dengan panjang variabel, yaitu 128 bit, 192 bit, dan 256 bit. Implementasi enkripsi AES akan mengubah data sensitif menjadi ciphertext yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai, sehingga meningkatkan keamanan data. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem pendaftaran berbasis web yang mengamankan formulir data siswa di SPS Tapos menggunakan metode AES.

Hasil dari penelitian ini menunjukkan bahwa sistem yang diusulkan mampu memberikan tingkat keamanan yang memadai, sesuai dengan kebutuhan lembaga pendidikan, dan efektif dalam melindungi data siswa dari potensi penyalahgunaan. Dengan adanya sistem ini, diharapkan keamanan data siswa dapat lebih terjamin dan proses pendaftaran dapat dilakukan dengan lebih aman dan efisien.

Kata Kunci : AES, Enkripsi, Dekripsi, Keamanan data

DAFTAR ISI

ABSTRAK.....	iv
KATA PENGANTAR	vi
DAFTAR ISI	ix
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	6
1.3 Batasan Masalah.....	6
1.4 Tujuan Penelitian	7
1.5 Manfaat Penelitian	7
BAB II TINJAUAN PUSTAKA	8
2.1 Studi Literatur	8
2.2 Landasan Teori.....	15
2.2.1 Keamanan Data.....	16
2.2.2 <i>Website</i>	16
2.2.3 Kriptografi <i>Advanced Encryption Standard</i> (AES).....	17
2.2.4 Enkripsi Algoritma Advanced Encryption Standard (AES 128).	20
2.2.5 Dekripsi Algoritma Advanced Encryption Standard (AES 128)	23
2.2.6 Pengujian AES.....	27
BAB III METODOLOGI PENELITIAN	31
3.1 Metode Penelitian	31
3.2 Alur Penelitian	32
3.2.1 Pengumpulan Data(<i>Requirement</i>)	33
3.2.2 Analisa Kebutuhan Sistem (<i>Design</i>)	35
3.2.3 Rancangan Sistem.....	37

3.2.4 Desain Sistem Aplikasi	39
3.2.5 Rancangan <i>Wireframe</i>	44
3.2.6 <i>Implementation</i>	56
3.2.7 <i>Testing</i>	57
3.2.8 <i>Maintenance</i>	59
BAB IV HASIL DAN PEMBAHASAN.....	60
4.1 Spesifikasi kebutuhan	60
4.1.1 Alat dan Bahan.....	60
4.2 Implementasi Hasil.....	61
4.2.1 Tampilan Halaman Utama	61
4.2.2 Tampilan Halaman Pendaftaran Siswa	62
4.2.3 Tampilan Halaman Siswa Berhasil Daftar	63
4.2.4 Tampilan Halaman Admin	64
4.2.5 Tampilan Berkas Enkripsi	69
4.3 Pengujian sistem	72
4.4 Pengujian Avalanche Effect.....	78
4.5 Pengujian Character Error Rate	80
4.6 Pengujian Black Box testing	82
BAB V PENUTUP	85
5.1 Kesimpulan.....	85
5.2 Saran	86
DAFTAR PUSTAKA	89
LAMPIRAN	96

DAFTAR TABEL

Tabel 2. 1 Tabel Penelitian Terdahulu	12
Tabel 2. 2 Perbandingan Jumlah Round dan Key	19
Tabel 4. 1 Pengujian Format Word	73
Tabel 4. 2 Pengujian Format PDF	74
Tabel 4. 3 Pengujian Format Excel	75
Tabel 4. 4 Pengujian Format jpg	76
Tabel 4. 5 Pengujian <i>Avalanche Effect</i>	79
Tabel 4. 6 Pengujian Character Error Rate	81
Tabel 4. 7 Pengujian Black Box Testing	83

DAFTAR GAMBAR

Gambar 2. 1 Enkripsi dan Dekripsi	18
Gambar 2. 2 Ilustrasi proses enkripsi AES.....	21
Gambar 2. 3 proses algoritma dekripsi AES.....	23
Gambar 3. 1 Metode waterfall	32
Gambar 3. 2 Context Diagram.....	37
Gambar 3. 3 DFD Level 1	38
Gambar 3. 4 Rancangan Alur Sistem Aplikasi	40
Gambar 3. 5 Activity Diagram Pendaftaran	41
Gambar 3. 6 Activity Diagram Proses Enkripsi	42
Gambar 3. 7 Activity Diagram Proses Dekripsi	43
Gambar 3. 8 Desain halaman utama	44
Gambar 3. 9 Desain halaman pendaftaran	45
Gambar 3. 10 Desain halaman berhasil daftar	46
Gambar 3. 11 Desain halaman login admin	47
Gambar 3. 12 Desain beranda (dashboard)	48
Gambar 3. 13 Desain halaman enkripsi	49
Gambar 3. 14 Desain halaman dekripsi	50
Gambar 3. 15 Desain halaman file	52
Gambar 3. 16 Desain halaman pendaftar	53
Gambar 3. 17 Desain halaman tentang.....	54
Gambar 4. 1 Tampilan Halaman Utama	61
Gambar 4. 2 Tampilan Halaman Pendaftaran.....	62
Gambar 4. 3 Tampilan Halaman Berhasil daftar	63
Gambar 4. 4 Berkas bukti pendaftaran.....	63
Gambar 4. 5 Tampilan Halaman Login Admin	64
Gambar 4. 6 Tampilan Halaman Dashboard.....	64
Gambar 4. 7 Tampilan Menu Enkripsi	65
Gambar 4. 8 Tampilan Menu Dekripsi.....	66
Gambar 4. 9 Tampilan Proses Dekripsi.....	67
Gambar 4. 10 Tampilan Menu File.....	67
Gambar 4. 11 tampilan Menu Data Pendaftar	68

Gambar 4. 12 Tampilan Menu Tentang	69
Gambar 4. 13 Tampilan berkas sebelum dienkripsi	70
Gambar 4. 14 Tampilan berkas setelah terenkripsi	71