

ANALISIS PERBANDINGAN ALGORITMA AES RIJNDAEL DAN SERPENT PADA CITRA DIGITAL

Reyza Rizky Rozitya

(13.04.112.00123)

Pembimbing 1 : Yoga Dwitya Pramudita, S.Kom., M.Cs.

Pembimbing 2 : Dwi Kuswanto, S.Pd., M.T.

ABSTRAK

Keamanan data sangatlah penting pada zaman yang modern ini, teknologi semakin berkembang, transfer informasi pun menjadi lebih mudah dengan internet. Namun banyaknya kejahatan di dunia maya pun juga semakin bertambah. Oleh karena itu untuk melindungi data terhadap akses, pengubahan dan penghalangan dari pihak yang tidak berwenang, maka dibuatla suatu teknik untuk mengamankan data. Salah satu teknik yang dapat digunakan untuk pengamanan data yaitu dengan menerapkan metode enkripsi. Pada penelitian ini metode enkripsi yang digunakan adalah *AES Rijndael* dan *Serpent*. Hasil dari uji coba performa kecepatan enkripsi didapatkan nilai rata-rata **167.6 second** untuk *AES Rijndael* dan **5651.4 second** untuk *Serpent*, sedangkan kecepatan dekripsi **205.8 second** untuk *AES Rijndael* dan **595.4 second** untuk *Serpent*. hasil pengujian *MSE* didapatkan nilai rata-rata **16407.4** untuk *AES Rijndael* dan **16393.8** untuk *Serpent*, hasil pengujian *PSNR* didapatkan nilai rata-rata **6.497544 db** untuk *AES Rijndael* dan **6.502172 db** untuk *Serpent*, hasil pengujian *NPCR* didapatkan nilai rata-rata **92.35544%** untuk *AES Rijndael* dan **92.4974%** untuk *Serpent*, sedangkkan hasil pengujian *UACI* didapatkan nilai rata-rata **42.39498%** untuk *AES Rijndael* dan **42.3816%** untuk *Serpent*.

Kata Kunci : *AES Rijndael*, *Serpent*, Performa kecepatan, *MSE*, *PSNR*, *NPCR*, *UACI*

**COMPARATIVE ANALYSIS OF AES RIJNDAEL AND SERPENT
ALGORITHM IN DIGITAL IMAGE**

Reyza Rizky Rozitya

(13.04.112.00123)

Pembimbing 1 : Yoga Dwitya Pramudita, S.Kom., M.Cs.

Pembimbing 2 : Dwi Kuswanto, S.Pd., M.T.

ABSTRACT

*Data security is very important in this modern era, technology is increasingly developing, information transfer becomes easier with the internet. But the amount of crime in cyberspace is also increasing. Therefore to protect data against access, alteration and deterrence from unauthorized parties, then a technique is created to secure data. One technique that can be used for data security is to apply the encryption method. In this study the encryption method used is AES Rijndael and Serpent. The results of the encryption speed performance test obtained an average value of **167.6** second for AES Rijndael and **5651.4** second for Serpent, while decryption speed **205.8** second for AES Rijndael and **595.4** second for Serpent. MSE test results obtained an average value of **16407.4** for AES Rijndael and **16393.8** for Serpent, the PSNR test results obtained an average value of **6.497544** db for AES Rijndael and **6.502172** db for Serpent, the NPCR test results obtained an average value of **92,35544%** for AES Rijndael and **92.4974%** for Serpent, while the UACI test results obtained an average value of **42.39498%** for AES Rijndael and **42.3816%** for Serpent.*

Keywords : AES Rijndael, Serpent, Speed Performance, MSE, PSNR, NPCR, UACI

DAFTAR ISI

HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN ORISINALITAS	iii
ABSTRAK.....	iv
DAFTAR ISI	v
DAFTAR GAMBAR.....	vii
DAFTAR TABEL	viii
DAFTAR LAMPIRAN	ix
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Perumusan Masalah	2
1.2.1. Permasalahan.....	2
1.3. Tujuan Dan Manfaat	2
1.3.1. Tujuan Penelitian.....	2
1.3.2. Manfaat Penelitian	2
1.4. Batasan Masalah	2
1.5. Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA	4
2.1. PENELITIAN SEBELUMNYA	4
2.2. LANDASAN TEORI.....	7
2.2.1. PENGERTIAN KRIPTOGRAFI.....	7
2.2.2. KRIPTOGRAFI KUNCI SIMETRI	7
2.2.3. Block Cipher	8
2.3. ALGORITMA KRIPTOGRAFI.....	8
2.3.1. AES Rijndael	8
2.3.2. <i>Serpent</i>	10
2.4. Bahasa Pemrograman Matlab.....	12
2.5. Parameter yang digunakan	15
5. Metodologi Penelitian	17
BAB III METODE USULAN	18
3.1. Desain Perancangan Sistem	18

3.1.1.	Flowchart <i>AES Rijndael</i>	18
3.1.2.	Flowchart <i>Serpent</i>	19
3.1.3.	Flowchart Aplikasi	20
3.1.4.	Menu Aplikasi	20
3.2.	Skenario Uji Coba	21
BAB IV HASIL DAN PEMBAHASAN.....		24
4.1.	Batasan Implementasi	24
4.1.1.	Spesifikasi Perangkat Keras	24
4.1.2.	Spesifikasi Perangkat Lunak	24
4.2.	Implementasi Tampilan Program	24
4.3.	Implementasi Kode	32
4.2.1	Implementasi Algoritma <i>AES Rijndael</i>	33
4.2.2	Implementasi Algoritma <i>Serpent</i>	46
4.4.	Uji coba	58
4.4.1.	Uji coba Enkripsi dan dekripsi	58
4.4.2.	Uji coba Performa Kecepatan(<i>TIME</i>)	61
4.4.3.	Uji coba Mean Squared Error(<i>MSE</i>)	64
4.4.4.	Uji coba <i>Peak Signal to Noise Ratio (PSNR)</i>	65
4.4.5.	Uji coba <i>Number of Pixel Changed Rate(NPCR)</i>	66
4.4.6.	Uji coba <i>Unified Average Change Intensity (UACI)</i>	67
BAB V PENUTUP		68
5.1.	Kesimpulan	68
5.2.	Saran	69
DAFTAR PUSTAKA.....		70
LAMPIRAN		72
TENTANG PENULIS.....		99

DAFTAR GAMBAR

Gambar 2.1. Diagram Alur AES Rijndael	9
Gambar 2.2. Diagram Alur Serpent	11
Gambar 2.3. Skema Algoritma Serpent	12
Gambar 3.1. Flowcart AES Rijndael	18
Gambar 3.2. Flowchart Serpent.....	19
Gambar 3.3. Flowchart Aplikasi.....	20
Gambar 4.1. Tampilan Utama	25
Gambar 4.2. Tombol Browse	25
Gambar 4.3. Memilih file	26
Gambar 4.4. Citra Awal	26
Gambar 4.5. Tampilan Setelah Citra Dipilih.....	27
Gambar 4.6. Kolom Key	27
Gambar 4. 7 Tombol Enkripsi	28
Gambar 4.8. Tampilan Setelah Enkripsi	28
Gambar 4.9. Hasil Enkripsi <i>AES Rijndael</i>	29
Gambar 4.10. Hasil Enkripsi <i>Serpent</i>	29
Gambar 4.11. Tampilan Parameter hasil Enkripsi <i>AES Rijndael</i>	30
Gambar 4.12. Tampilan Parameter hasil Dekripsi <i>AES Rijndael</i>	30
Gambar 4.13. Tombol Dekripsi.....	31
Gambar 4.14. Tampilan Setelah Dekripsi	31
Gambar 4.15. Hasil Dekripsi <i>AES Rijndael</i>	32
Gambar 4.16. Tombol Reset.....	32

DAFTAR TABEL

Tabel 2.1. Format citra pada Matlab	13
Tabel 4.1. Citra Hasil Enkripsi	59
Tabel 4.2. Citra Hasil Dekripsi	60
Tabel 4.3. Jenis Dan Ukuran Data Uji	61
Tabel 4.4. Hasil Pengujian Kecepatan	62
Tabel 4.5. Selisih waktu Enkripsi algoritma <i>AES Rijndael</i> dengan <i>Serpent</i>	63
Tabel 4.6. Selisih waktu Dekripsi algoritma <i>AES Rijndael</i> dengan <i>Serpent</i>	63
Tabel 4.7. Uji coba <i>Mean Squared error</i> pada citra hasil enkripsi	64
Tabel 4.8. Selisih nilai MSE algoritma <i>AES Rijndael</i> dengan <i>Serpent</i>	64
Tabel 4.9. Uji coba <i>Peak Signal to Noise Ratio</i> pada citra hasil enkripsi	65
Tabel 4.10. Selisih nilai <i>PSNR</i> algoritma <i>AES Rijndael</i> dengan <i>Serpent</i>	65
Tabel 4.11. Uji coba <i>Number of Pixel Change Rate</i> hasil enkripsi	66
Tabel 4.12. Selisih nilai <i>NPCR</i> algoritma <i>AES RIjndael</i> dengan <i>Serpent</i>	66
Tabel 4.13. Uji coba <i>Unified Average Change Intensity</i> hasil enkripsi	67
Tabel 4.14 Selisih nilai <i>UACI</i> algoritma <i>AES Rijndael</i> dengan <i>Serpent</i>	67

DAFTAR LAMPIRAN

Lampiran 1 : <i>Source Code</i> Fungsi utama Enkripsi <i>AES Rijndael</i>	72
Lampiran 2 : <i>Source Code</i> Fungsi <i>Cipher</i>	75
Lampiran 3 : <i>Source Code</i> Fungsi <i>Key Expansion 128bit</i>	76
Lampiran 4 : <i>Source Code</i> Fungsi <i>Key Expansion 192bit</i>	77
Lampiran 5 : <i>Source Code</i> Fungsi <i>Key Expansion 256bit</i>	78
Lampiran 6 : <i>Source Code</i> <i>S-Box</i>	79
Lampiran 7 : <i>Source code</i> Fungsi <i>Mix Column</i>	82
Lampiran 8 : <i>Source code</i> Fungsi <i>Inverse Cipher</i>	83
Lampiran 9 : <i>Source code</i> Fungsi utama Dekripsi <i>AES Rijndael</i>	84
Lampiran 10 : <i>Source code</i> Fungsi utama <i>Serpent</i>	87
Lampiran 11 : <i>Source code</i> Fungsi <i>Cipher Serpent</i>	90
Lampiran 12 : <i>Source code</i> Fungsi <i>Key Expansion 256 Serpent</i>	91
Lampiran 13 : <i>Source code</i> Fungsi <i>Shift</i>	92
Lampiran 14 : <i>Source code</i> <i>Xor</i>	93
Lampiran 15 : <i>Source code</i> Fungsi <i>Inverse Cipher Serpent</i>	95
Lampiran 16 : <i>Source code</i> Fungsi utama Dekripsi <i>Serpent</i>	96