

DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR.....	i
LEMBAR PENGESAHAN PENGUJI SIDANG TUGAS AKHIR.....	ii
LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR.....	iii
<i>ABSTRACT</i>	iv
ABSTRAK	v
MOTTO DAN PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR.....	xiv
BAB I PENDAHULUAN.....	I-1
1.1 Latar Belakang	I-1
1.2 Rumusan Masalah	I-6
1.3 Tujuan Penelitian.....	I-7
1.4 Manfaat Penelitian.....	I-7
1.5 Batasan Masalah.....	I-7
1.6 Sistematika Penulisan.....	I-8
BAB II TINJAUAN PUSTAKA.....	II-1
2.1 Landasan Teori	II-1
2.1.1 Kriptografi	II-1
2.1.2 <i>Advanced Encryption Standard (AES-128)</i>	II-1
2.1.3 Block cipher dan Cipher Block Chaining.....	II-3
2.1.4 <i>Bit permutation</i>	II-3
2.1.5 <i>Logistic chaotic map</i>	II-5
2.1.6 <i>Fisher-Yates shuffle</i>	II-6
2.1.7 Difusi <i>Ciphertext</i>	II-7
2.2 Parameter Pengujian.....	II-8
2.2.1 Kecepatan Enkripsi	II-8
2.2.2 Kecepatan Dekripsi.....	II-9
2.2.3 <i>Avalanche effect</i>	II-9

2.2.4 <i>Throughput</i>	II-10
2.2.5 Entropi Shannon	II-10
2.2.6 <i>Key sensitivity</i>	II-11
2.2.7 <i>Frequency test</i>	II-12
2.2.8 <i>Runs test</i>	II-12
2.2.9 <i>Chi-Square test</i>	II-13
2.3 State of The Art	II-14
2.4 Matriks Penelitian.....	II-17
BAB III METODOLOGI	III-1
3.1. Metodologi Penelitian	III-1
3.2. Lingkungan Pengujian	III-1
3.3. Pembangkitan Tabel Permutasi Dinamis	III-2
3.4. Proses Enkripsi-Dekripsi.....	III-7
3.5. Alur Penelitian	III-18
3.5.1. Studi Literatur	III-19
3.5.2. Identifikasi Masalah	III-20
3.5.3. Perancangan dan Implementasi Algoritma.....	III-21
3.5.4. Pengujian dan Evaluasi	III-22
3.5.5. Penarikan Kesimpulan	III-27
BAB IV HASIL DAN PEMBAHASAN	IV-1
4.1 Hasil Pengujian Enkripsi	IV-1
4.1.1 Hasil Pengujian Validitas Enkripsi	IV-1
4.1.2 Hasil Pengujian Kecepatan Enkripsi.....	IV-2
4.1.3 Hasil Pengujian <i>Throughput</i> Enkripsi.....	IV-2
4.2 Hasil Pengujian Dekripsi	IV-3
4.2.1 Hasil Uji Validitas Dekripsi	IV-3
4.2.2 Hasil Uji Kecepatan Dekripsi	IV-4
4.2.3 Hasil Pengujian <i>Throughput</i> Dekripsi	IV-5
4.3 Hasil Pengujian <i>Avalanche effect</i>	IV-5
4.4 Hasil Pengujian Entropi Shannon.....	IV-6
4.5 Hasil Pengujian <i>Key sensitivity</i>	IV-7

4.6 Hasil Pengujian <i>Frequency test</i>	IV-8
4.7 Hasil Pengujian <i>Runs test</i>	IV-8
4.8 Hasil Pengujian <i>Chi-Square test</i>	IV-9
4.9 Hasil Pengujian Perbandingan.....	IV-9
4.9.1 Hasil Pengujian Kecepatan Enkripsi.....	IV-10
4.9.2 Hasil Pengujian Kecepatan Dekripsi	IV-13
4.9.3 Hasil Pengujian <i>Throughput</i>	IV-17
4.9.4 Hasil Pengujian <i>Avalanche effect</i>	IV-22
4.9.5 Hasil Pengujian Entropi Shannon	IV-23
4.9.6 Hasil Pengujian <i>Key sensitivity</i>	IV-25
4.9.7 Hasil Pengujian <i>Frequency test</i>	IV-26
4.9.8 Hasil Pengujian <i>Runs test</i>	IV-27
4.9.9 Hasil Pengujian <i>Chi-Square test</i>	IV-28
4.10 Pembahasan	IV-29
4.10.1 Kecepatan Enkripsi dan Dekripsi	IV-30
4.10.2 <i>Throughput</i> Enkripsi dan Dekripsi.....	IV-31
4.10.3 <i>Avalanche effect</i>	IV-31
4.10.4 Entropi Shannon	IV-32
4.10.5 <i>Key sensitivity</i>	IV-32
4.10.6 Pengujian Statistik (<i>Frequency test</i> , <i>Runs test</i> , dan <i>Chi-Square test</i>)	IV-32
4.10.7 Analisis <i>Trade off</i> dengan Penelitian Terdahulu	IV-33
4.10.8 Keterbatasan Hasil Pengujian	IV-41
BAB V KESIMPULAN DAN SARAN	V-1
5.1 Kesimpulan.....	V-1
5.2 Saran	V-2
DAFTAR PUSTAKA	119
LAMPIRAN.....	L1

DAFTAR TABEL

Tabel 2.1. State of The Art	II-14
Tabel 2.2. Matriks Penelitian	II-17
Tabel 3.1. Spesifikasi Perangkat Keras dan Perangkat Lunak	III-2
Tabel 4.1. Hasil Pengujian Uji Validitas Enkripsi	IV-1
Tabel 4.2. Hasil Pengujian Kecepatan Enkripsi	IV-2
Tabel 4.3. Hasil Pengujian <i>Throughput</i> Enkripsi	IV-2
Tabel 4.4. Hasil Pengujian Uji Validitas Dekripsi	IV-3
Tabel 4.5. Hasil Pengujian Kecepatan Dekripsi	IV-4
Tabel 4.6. Hasil Pengujian <i>Throughput</i> Dekripsi	IV-5
Tabel 4.7. Hasil Pengujian <i>Avalanche effect</i>	IV-5
Tabel 4.8. Hasil Pengujian Entropi Shannon	IV-6
Tabel 4.9. Hasil Pengujian <i>Key sensitivity</i>	IV-7
Tabel 4.10. Hasil Pengujian <i>Frequency test</i>	IV-8
Tabel 4.11. Hasil Pengujian <i>Runs test</i>	IV-8
Tabel 4.12. Hasil Pengujian <i>Chi-Square test</i>	IV-9
Tabel 4.13. Hasil Pengujian Komparasi Kecepatan Enkripsi	IV-10
Tabel 4.14. Hasil Pengujian Komparasi Kecepatan Dekripsi	IV-13
Tabel 4.15. Hasil Pengujian Komparasi <i>Throughput</i> Enkripsi	IV-17
Tabel 4.16. Hasil Pengujian Komparasi <i>Throughput</i> Dekripsi	IV-19
Tabel 4.17. Hasil Pengujian Komparasi <i>Avalanche effect</i>	IV-22
Tabel 4.18. Hasil Pengujian Komparasi Entropi Shannon	IV-23
Tabel 4.19. Hasil Pengujian Komparasi <i>Key sensitivity</i>	IV-25
Tabel 4.20. Hasil Pengujian Komparasi <i>Frequency test</i>	IV-26
Tabel 4.21. Hasil Pengujian Komparasi <i>Runs test</i>	IV-27
Tabel 4.22. Hasil Pengujian Komparasi <i>Chi-Square test</i>	IV-28
Tabel 4.23. Tabel Ringkas Hasil Pengujian	IV-33
Tabel 4.24. Tabel Ringkas Hasil Pengujian	IV-34

DAFTAR GAMBAR

Gambar 2.1 Diagram Proses AES	II-2
Gambar 2.2. Proses <i>Bit permutation</i> (sumber: researchgate).....	II-4
Gambar 2.3. Proses <i>Fisher-Yates shuffle</i> (sumber: springer.com)	II-6
Gambar 3.1. Pembangkitan tabel permutasi dinamis.....	III-6
Gambar 3.2. Usulan Proses Enkripsi-Dekripsi	III-7
Gambar 3.3. Alur Penelitian.....	III-19
Gambar 4.1 Grafik Hasil Pengujian Kecepatan Enkripsi 10-50KB.....	IV-12
Gambar 4.2 Grafik Hasil Pengujian Kecepatan Enkripsi 100KB-1MB	IV-12
Gambar 4.3 Grafik Hasil Pengujian Kecepatan Dekripsi 10-50KB	IV-15
Gambar 4.4 Grafik Hasil Pengujian Kecepatan Dekripsi 100KB-1MB	IV-15
Gambar 4.5 Grafik Hasil Pengujian <i>Throughput</i> Enkripsi.....	IV-18
Gambar 4.6 Grafik Hasil Pengujian <i>Throughput</i> Dekripsi	IV-21
Gambar 4.7 Grafik Hasil Pengujian <i>Avalanche effect</i>	IV-22
Gambar 4.8 Grafik Hasil Pengujian Entropi Shannon	IV-24
Gambar 4.9 Grafik Hasil Pengujian <i>Key sensitivity</i>	IV-25
Gambar 4.10 Grafik Hasil Pengujian <i>Frequency test</i>	IV-26
Gambar 4.11 Grafik Hasil Pengujian <i>Runs test</i>	IV-28
Gambar 4.12 Grafik Hasil Pengujian <i>Chi-Square test</i>	IV-29