



DAFTAR ISI

DAFTAR ISI.....	i
DAFTAR GAMBAR.....	iv
DAFTAR TABEL.....	vi
KATA PENGANTAR.....	vii
INTISARI.....	ix
ABSTRACT.....	x
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
1.6 Metodologi Penelitian.....	4
1.6.1 Metode Pengumpulan Data.....	5
1.6.2 Metode Analisis Data.....	5
1.7 Sistematika Penulisan.....	5
BAB II TINJAUAN PUSTAKA.....	7
BAB III LANDASAN TEORI.....	12
3.1 Kriptografi.....	12
3.1.1 Enkripsi dan Dekripsi Kriptografi.....	12
3.1.2 <i>Cipher</i>	13
3.2 Kriptosistem.....	13
3.3 Confusion and Diffusion.....	14
3.4 Advanced Encryption Standard.....	14
3.5.1 <i>SubBytes</i>	15
3.5.2 <i>ShiftRows</i>	15
3.5.4 <i>AddRoundKey</i>	17
3.6 Iterated Function System.....	17



3.7 Cryptoanalysis.....	19
3.8 <i>Avalanche Effect</i>	19
3.9 Kolmogorov –Smirnov Test.....	20
BAB IV METODE PENELITIAN.....	21
4.1 Alat dan Bahan.....	21
4.2 Deskripsi Umum Penelitian.....	21
4.3 Tahapan Penelitian.....	22
4.4 Algoritma IFS pada Kriptografi.....	23
4.5 Rancangan AES-IFS.....	26
4.5.1 Rancangan AES-IFS Sistem A.....	27
4.5.2 Rancangan AES-IFS Sistem B.....	27
4.5.3 Rancangan AES-IFS Sistem C.....	28
4.5.4 Rancangan AES-IFS Sistem D.....	28
4.5.5 Rancangan AES-IFS Sistem E.....	29
4.6 Tahap IFS.....	29
4.7 Rancangan Program.....	30
BAB V IMPLEMENTASI.....	32
5.1 Implementasi.....	32
5.1.1 Implementasi Perangkat Lunak.....	32
5.2 Implementasi Python.....	32
5.2.1 Inisialisasi Substitution Box.....	33
5.2.2 Inisialisasi IFS.....	34
5.2.3 Fungsi Pengubah Data-Type.....	34
5.2.4 Fungsi tahap Enkripsi S-Box.....	35
5.2.5 Fungsi tahap Enkripsi <i>ShiftRows</i>	35
5.2.6 Galois Field.....	36
5.2.7 Fungsi tahap Enkripsi <i>MixColumn</i>	37
5.2.8 Fungsi tahap Enkripsi <i>mixColumn</i>	37



5.2.9 Fungsi tahap Enkripsi Iterated Function System.....	38
5.2.10 Eksekusi Program.....	39
5.2.11 Analisis Enkripsi.....	40
BAB VI HASIL DAN PEMBAHASAN.....	41
6.1 Deskripsi Data.....	41
6.2 Pembahasan Hasil Enkripsi.....	42
6.3 Pembahasan Hasil Dekripsi.....	42
6.4 Analisis Avalanche Effect.....	43
6.5 Analisis Kolmogorov Smirnov Test.....	44
6.6 Analisis Frequency Test.....	44
6.7 Runtime.....	45
6.8 Analisis Hasil Pengujian.....	46
BAB VII KESIMPULAN.....	48
7.1 Hasil Akhir.....	48
7.2 Saran Penelitian Selanjutnya.....	48
DAFTAR PUSTAKA.....	49
LAMPIRAN.....	50