

DAFTAR ISI

TUGAS AKHIR.....	i
LEMBAR PERSETUJUAN.....	ii
LEMBAR PERNYATAAN ORISINALITAS	iii
UCAPAN TERIMA KASIH.....	iv
ABSTRAK	v
ABSTRACT.....	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xii
DAFTAR SINGKATAN	xiii
BAB I	14
PENDAHULUAN	14
1.1 Latar Belakang	14
1.2 Rumusan Masalah	15
1.3 Tujuan.....	15
1.4 Batasan Masalah.....	16
1.5 Metodologi Penelitian	16
1.6 Sistematika Penulisan.....	17
BAB II.....	18
DASAR TEORI.....	18
2.1 Black Box	18
2.2 Flight Data Recorder.....	18
2.3 Kriptografi.....	20

2.4	Stream Cipher Variably Modified Permutation Composition (VMPC) .	21
2.4.1	Definisi dari fungsi VMPC[6]	22
2.4.2	Key Scheduling Algorithm	23
2.4.3	Pseudo-Random Generation Algorithm	24
BAB III		26
PERANCANGAN.....		26
3.1	Analisis Kebutuhan	26
3.2	Gambaran Umum Sistem	26
3.3	Perancangan Sistem	27
3.3.1	Diagram Alir Proses Enkripsi.....	28
3.3.2	Diagram Alir Proses Dekripsi.....	29
3.4	Uji Performansi.....	30
BAB IV		31
IMPLEMENTASI DAN PENGUJIAN SISTEM		31
4.1	Implementasi Sistem.....	31
4.2	Pengujian Performansi.....	31
4.2.1	Pengujian Waktu Enkripsi.....	31
4.2.2	Pengujian Waktu Dekripsi	36
4.2.3	Pengujian Keamanan Sistem.....	41
4.2.4	Pengujian Keutuhan Data.....	44
BAB V		46
KESIMPULAN DAN SARAN		46
5.1	Kesimpulan	46
5.2	Saran.....	47
DAFTAR PUSTAKA.....		48
LAMPIRAN A		49

Hasil Pengujian Keutuhan Data	50
LAMPIRAN B	54
Hasil Pengujian Avalanche Effect	55
Cuplian Bit Hasil Pengujian <i>Avalanche Effect</i> Kunci Sama.....	69