

DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS	iii
ABSTRAK	iv
<i>ABSTRACT</i>	v
KATA PENGANTAR.....	vi
UCAPAN TERIMA KASIH.....	vii
DAFTAR ISI	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
DAFTAR RUMUS.....	xiii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah.....	3
1.3. Tujuan Penelitian	3
1.4. Batasan Masalah	3
1.5. Manfaat Penelitian	3
1.6. Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	6
2.1. Penelitian Terdahulu	6
2.2. Kriptografi	9
2.3. Twofish.....	10
2.4. Kyber Key Encapsulation Mechanism (KEM).....	11
2.5. Hybrid Encryption	13
2.6. Alasan Pemilihan Teori / Model / Kerangka Kerja	15
BAB III METODOLOGI PENELITIAN	17
3.1. Jenis Penelitian	17
3.2. Alat dan Bahan	17
3.3. Rancangan Penelitian	18
3.3.1. Proses Key Generation Kyber KEM	19
3.3.2. <i>Encapsulation Mechanism</i>	20
3.3.3. Proses Enkripsi <i>File Twofish</i>	21
3.3.4. Decapsulation	22
3.3.5. Proses Dekripsi <i>File Twofish</i>	23

3.4.	Pengujian Sistem	24
3.5.	Evaluasi Performa.....	26
3.6.	Desain Sistem	27
3.7.	Jadwal Penelitian	28
BAB IV HASIL DAN PEMBAHASAN		30
4.1.	Implementasi	30
4.1.1.	Bahasa dan <i>Library</i> Pemrograman	30
4.1.2.	Struktur Sistem.....	30
4.1.3.	Implementasi UI/UX.....	42
4.2.	Hasil Pengujian	44
4.2.1.	Pengujian Berdasarkan Format <i>File</i> dan <i>File Size</i>	44
4.2.2.	Pengujian pada Lingkungan VM to VM	49
4.2.3.	Pengujian Kyber KEM dan AES	51
4.2.4.	Pengujian Sniffing Wireshark	53
4.2.5.	Analisis Hash Values.....	55
4.3.	Pembahasan.....	58
4.3.1.	Arsitektur dan Mekanisme Sistem Hybrid Encryption	58
4.3.2.	Evaluasi Kinerja Sistem.....	58
4.3.3.	Kelebihan dan Kekurangan Sistem.....	60
BAB V KESIMPULAN DAN SARAN		62
5.1.	Kesimpulan.....	62
5.2.	Saran.....	63
DAFTAR PUSTAKA		64