

DAFTAR ISI

| | |
|--|------|
| LEMBAR PENGESAHAN | i |
| ABSTRAKSI | iv |
| ABSTRACT..... | v |
| KATA PENGANTAR..... | vi |
| LEMBAR PERSEMBAHAN..... | vii |
| DAFTAR ISI..... | viii |
| DAFTAR TABEL | x |
| DAFTAR GAMBAR..... | xi |
| DAFTAR SINGKATAN..... | xii |
| DAFTAR ISTILAH | xiii |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Tujuan Penelitian | 2 |
| 1.3 Rumusan Masalah..... | 2 |
| 1.4 Batasan Masalah..... | 2 |
| 1.5 Metodologi Penelitian..... | 3 |
| 1.6 Sistematika Penulisan | 3 |
| BAB II DASAR TEORI..... | 5 |
| 2.1 Kriptografi | 5 |
| 2.2 Algoritma Simetris dan Asimetris | 6 |
| 2.2.1 Algoritma Simetris..... | 6 |
| 2.2.2 Algoritma Asimetris..... | 7 |
| 2.3 <i>Block Cipher</i> dan <i>Stream Cipher</i> | 7 |
| 2.3.1 <i>Block Cipher</i> | 7 |
| 2.3.2 <i>Stream Cipher</i> | 8 |
| 2.4 Algoritma DES..... | 8 |
| BAB III PERANCANGAN SISTEM | 10 |
| 3.1 Model Sistem..... | 10 |
| 3.1.1 Enkripsi DES Murni..... | 10 |

| | |
|---|-----------|
| 3.1.2 Dekripsi DES Murni | 11 |
| 3.1.3 M-DES..... | 12 |
| 3.2 Performa Sistem | 14 |
| 3.2.1 <i>Avalanche Effect</i> | 14 |
| 3.2.2 Waktu Komputasi..... | 14 |
| 3.3 Skema Pengujian | 15 |
| BAB IV ANALISIS HASIL SIMULASI..... | 16 |
| 4.1 Analisis Kebutuhan | 16 |
| 4.2 Pengujian Sistem | 16 |
| 4.2.1 Skenario Pengujian Sistem..... | 16 |
| 4.3 Hasil Pengujian | 17 |
| 4.3.1 Data Uji..... | 17 |
| 4.3.2 Pengujian Dengan Mengganti Komposisi Kunci 80-bit | 17 |
| 4.3.3 Pengujian Dengan Mengganti Komposisi Kunci 64-bit | 18 |
| 4.3.4 Pengujian Dengan Mengganti Input | 18 |
| BAB V KESIMPULAN DAN SARAN..... | 20 |
| 5.1 Kesimpulan | 20 |
| 5.2 Saran..... | 20 |
| DAFTAR PUSTAKA..... | 21 |