

## DAFTAR ISI

|                                                         |      |
|---------------------------------------------------------|------|
| LEMBAR PENGESAHAN.....                                  | ii   |
| LEMBAR ORISINALITAS .....                               | iii  |
| ABSTRAK.....                                            | iv   |
| <i>ABSTRACT</i> .....                                   | v    |
| KATA PENGANTAR.....                                     | vi   |
| UCAPAN TERIMA KASIH.....                                | vii  |
| DAFTAR ISI.....                                         | viii |
| DAFTAR TABEL.....                                       | xi   |
| DAFTAR GAMBAR .....                                     | xiii |
| DAFTAR <i>SOURCE CODE</i> .....                         | xv   |
| DAFTAR RUMUS.....                                       | xvi  |
| BAB I PENDAHULUAN .....                                 | 1    |
| 1.1 Latar Belakang .....                                | 1    |
| 1.2 Rumusan Masalah .....                               | 4    |
| 1.3 Tujuan Penelitian .....                             | 4    |
| 1.4 Batasan dan Asumsi Penelitian .....                 | 4    |
| 1.5 Manfaat Penelitian .....                            | 5    |
| 1.5.1 Manfaat Akademis.....                             | 5    |
| 1.5.2 Manfaat Ilmiah .....                              | 5    |
| 1.6 Sistematika Penulisan .....                         | 5    |
| BAB II LANDASAN TEORI .....                             | 7    |
| 2.1 Literatur Terkait Teori.....                        | 7    |
| 2.2 Kajian Teori.....                                   | 9    |
| 2.2.1 Kriptografi.....                                  | 9    |
| 2.2.2 <i>AES (Advanced Encryption Standard)</i> .....   | 11   |
| 2.2.3 Chacha20 .....                                    | 17   |
| 2.2.4 Entropi .....                                     | 20   |
| 2.2.5 Alasan Pemilihan AES, ChaCha20, dan Entropi ..... | 21   |
| BAB III METODOLOGI PENELITIAN .....                     | 23   |
| 3.1 Sistematika Penyelesaian Masalah.....               | 23   |
| 3.2 Alat dan Bahan .....                                | 23   |

|                                   |                                                                     |     |
|-----------------------------------|---------------------------------------------------------------------|-----|
| 3.2.1                             | Alat .....                                                          | 23  |
| 3.2.2                             | Bahan .....                                                         | 24  |
| 3.3                               | Rancangan Penelitian .....                                          | 24  |
| 3.3.1                             | Studi Literatur .....                                               | 26  |
| 3.3.2                             | Pengumpulan Data .....                                              | 26  |
| 3.3.3                             | Implementasi Modifikasi AES .....                                   | 27  |
| 3.3.4                             | Implementasi Kombinasi <i>AES</i> Modifikasi- <i>ChaCha20</i> ..... | 30  |
| 3.3.5                             | Implementasi Antarmuka Pengguna (UI) .....                          | 34  |
| 3.3.6                             | Pengujian Algoritma .....                                           | 35  |
| 3.3.7                             | Analisis Hasil .....                                                | 38  |
| BAB IV HASIL DAN PEMBAHASAN ..... |                                                                     | 39  |
| 4.1                               | Implementasi Algoritma .....                                        | 39  |
| 4.1.1                             | Proses Input <i>File</i> .....                                      | 40  |
| 4.1.2                             | Implementasi AES Standar .....                                      | 40  |
| 4.1.3                             | Implementasi Algoritma <i>AES</i> yang Dimodifikasi .....           | 42  |
| 4.1.4                             | Implementasi Algoritma <i>ChaCha20</i> .....                        | 49  |
| 4.1.5                             | Implementasi Enkripsi Ganda ( <i>AESM</i> dan <i>ChaCha20</i> ) ..  | 51  |
| 4.1.6                             | Alasan Penggunaan Padding pada <i>AES</i> Modifikasi .....          | 55  |
| 4.1.7                             | Pemrosesan Data Berdasarkan Byte .....                              | 56  |
| 4.1.8                             | Implementasi Antarmuka Pengguna .....                               | 57  |
| 4.1.9                             | Pengujian Awal dan Evaluasi Sistem .....                            | 60  |
| 4.2                               | Hasil Pengujian .....                                               | 63  |
| 4.2.1                             | Hasil Pengujian Waktu Enkripsi dan Dekripsi .....                   | 64  |
| 4.2.2                             | Hasil Pengujian Kecepatan Enkripsi dan Dekripsi .....               | 83  |
| 4.2.3                             | Hasil Analisis Entropi .....                                        | 99  |
| 4.2.4                             | Pengujian Hash Value Hasil Dekripsi .....                           | 106 |
| 4.2.5                             | Tampilan Hasil Enkripsi dan Dekripsi .....                          | 109 |
| 4.3                               | Pembahasan .....                                                    | 111 |
| 4.3.1                             | Evaluasi Rata-Rata Waktu Enkripsi dan Dekripsi .....                | 111 |
| 4.3.2                             | Evaluasi Rata-Rata Kecepatan Enkripsi dan Dekripsi ..               | 113 |
| 4.3.3                             | Evaluasi Rata-Rata Entropi .....                                    | 115 |
| 4.3.4                             | Perbandingan Kinerja Algoritma Secara Keseluruhan ..                | 115 |
| BAB V KESIMPULAN DAN SARAN .....  |                                                                     | 117 |
| 5.1                               | Kesimpulan .....                                                    | 117 |

|                      |            |     |
|----------------------|------------|-----|
| 5.2                  | Saran..... | 117 |
| DAFTAR PUSTAKA ..... |            | 119 |