

**IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD  
(AES) UNTUK PENGAMANAN CITRA DIGITAL**

**SKRIPSI**

Oleh :

**Maulana Akbar**  
**71220915063**



**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS ISLAM SUMATERA UTARA  
MEDAN  
2024**

## KATA PENGANTAR

*Assalamu 'alaikum Warahmatullahi Wabarakatuh.*

Alhamdulillah Segala puji dan syukur penulis kirimkan kepada Allah Swt. Yang telah memberikan rahmat dan Karunia-Nya kepada penulis sehingga dapat menyelesaikan Skripsi ini yang berjudul “IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK PENGAMANAN CITRA DIGITAL”. Tidak lupa Shalawat beserta salam penulis kirimkan Kepada Nabi Besar Muhammad SAW. Beserta kepada keluarga dan para sahabatnya.

Skripsi ini merupakan hasil karya tulis ilmiah penulis yang telah penulis buat beberapa bulan di Universitas Islam Sumatera Utara. Dalam penyusunan skripsi ini penulis banyak mendapatkan arahan, bimbingan dan bantuan dari pihak lain berupa nasehat, materil dan spiritual, dan informasi secara langsung maupun tidak langsung.

Pada kesempatan ini penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Ibu Ir. Darlina Tanjung, M.T Selaku Dekan Fakultas Teknik UISU.
2. Bapak Mhd. Zulfansyuri Siambaton S.T.,M.Kom selaku ketua Program Studi Teknik Informatika UISU Sekaligus Pembimbing 1 Penulis.
3. Bapak Heri Santoso S.Kom.,M.Kom selaku Pembimbing 2 Penulis.
4. Bapak Khairuddin Nasution S.T.,M.Kom selaku Penguji 1 Penulis.
5. Bapak Rachmat Aulia S.Kom.,M.Kom selaku Penguji 2 Penulis.
6. Ibu Tasliyah Haramaini S.Si.,M.Kom selaku Penguji 3 Penulis.
7. Seluruh staff pengajar Jurusan Teknik Informatika UISU yang telah banyak memberikan ilmu kepada penulis selama masa perkuliahan.

8. Dan Semua Pihak yang tidak dapat penulis sebutkan satu persatu.

## Daftar Isi

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| KATA PENGANTAR .....                                            | ii  |
| ABSTRAK.....                                                    | iv  |
| Daftar Isi.....                                                 | v   |
| Daftar Tabel.....                                               | vii |
| BAB I .....                                                     | 1   |
| PENDAHULUAN .....                                               | 1   |
| 1.1.    Latar Belakang.....                                     | 1   |
| 1.2.    Rumusan Masalah .....                                   | 2   |
| 1.3.    Batasan Masalah.....                                    | 2   |
| 1.4.    Tujuan Penelitian .....                                 | 3   |
| 1.5.    Metode Penelitian .....                                 | 3   |
| 1.6.    Sistematika Penulisan.....                              | 4   |
| BAB II .....                                                    | 6   |
| LANDASAN TEORI .....                                            | 6   |
| 2.1    Kriptografi .....                                        | 6   |
| 2.2    Algoritma <i>Advance Encryption Standart</i> (AES) ..... | 7   |
| 2.3    Citra Digital.....                                       | 18  |
| 2.4 <i>Flowchart</i> .....                                      | 21  |
| 2.4    Python .....                                             | 23  |
| BAB III .....                                                   | 25  |
| METODE PENELITIAN.....                                          | 25  |
| 3.1    Metode Pengumpulan Data .....                            | 25  |
| 3.2    Rancangan Penelitian.....                                | 25  |
| 3.3 <i>Flowchart</i> Program .....                              | 26  |
| 3.3    Rancangan Antarmuka Aplikasi .....                       | 27  |
| BAB IV .....                                                    | 29  |
| HASIL DAN PEMBAHASAN.....                                       | 29  |
| 4.1    Implementasi Sistem.....                                 | 29  |
| 4.2    Pembahasan .....                                         | 35  |

Gambar 4.13 menunjukkan proses pemilihan gambar yang akan dikriptanalisis dengan menggunakan *bruteforce*. Kemudian pada saat kita memilih gambar yang akan kita akan kriptanalisis, dan kita masukkan nilai header hexanya, maka program akan menampilkan notifikasi sebagai berikut :.....37

**BAB V** .....39

**KESIMPULAN DAN SARAN**.....39

**5.1 Kesimpulan**.....39

**5.2 Saran** .....39

**Daftar Pustaka** .....40

## Daftar Tabel

|                                                               |    |
|---------------------------------------------------------------|----|
| <b>Tabel 2. 1</b> Putaran Kunci Algoritma AES .....           | 8  |
| <b>Tabel 2. 2</b> Tabel S-Box Lengkap (16 x 16) .....         | 10 |
| <b>Tabel 2. 3</b> Matriks Hasil Setelah Langkah Subbytes..... | 12 |
| <b>Tabel 2. 4</b> Hasil Mixcolumns .....                      | 12 |
| <b>Tabel 2. 5</b> Simbol Flowchart .....                      | 22 |

## Daftar Gambar

|                     |                                                                   |    |
|---------------------|-------------------------------------------------------------------|----|
| <b>Gambar 3. 1</b>  | Diagram Umum Enkripsi dan Dekripsi Pengamanan Citra Digital ..... | 25 |
| <b>Gambar 3. 2</b>  | Flowchart Sistem.....                                             | 26 |
| <b>Gambar 3. 3</b>  | Rancangan Interface Aplikasi Implementasi Algoritma (Aes).....    | 28 |
| <b>Gambar 4. 1</b>  | Tampilan Aplikasi Program.....                                    | 29 |
| <b>Gambar 4. 2</b>  | Contoh Gambar Yang Akan Dienkripsi.....                           | 30 |
| <b>Gambar 4. 3</b>  | Penguploadan Gambar .....                                         | 30 |
| <b>Gambar 4. 4</b>  | Respon Tombol Enkripsi Gambar .....                               | 31 |
| <b>Gambar 4. 5</b>  | Hasil Enkripsi .....                                              | 32 |
| <b>Gambar 4. 6</b>  | Detail ukuran gambar enkripsi .....                               | 32 |
| <b>Gambar 4. 7</b>  | Tampilan aplikasi .....                                           | 33 |
| <b>Gambar 4. 8</b>  | Pilihan Gambar Yang Akan Didekripsi .....                         | 33 |
| <b>Gambar 4. 9</b>  | Pengambilan kunci AES.....                                        | 34 |
| <b>Gambar 4. 10</b> | Notifikasi Program Telah Berhasil Dekripsi .....                  | 34 |
| <b>Gambar 4. 11</b> | Hasil Dekripsi Gambar .....                                       | 35 |

### **Daftar Pustaka**

- Agita, Y., Tarigan, P., Aulia, R., & Marwan, A. (2024). *Algoritma AES 128 dalam Mengenkripsikan Berkas Bansos Kecamatan Tigabinanga Berbasis Web*. 17(2), 2580–2582.
- Budiman, M. A., Rachmawati, D., & Syahnan, I. P. (2023). A tutorial on using ElGamal cryptosystem and RC4-P1 cipher in a hybrid scheme. *Journal of Physics: Conference Series*, 2421(1), 012033. <https://doi.org/10.1088/1742-6596/2421/1/012033>
- Gonzalez, R. C., & Woods, R. E. (2018). *4TH EDITION Digital image processing*.
- Katz, J., & Lindell, Y. (2021). *Introduction to Modern Cryptography* (Thrid Edit). Chapman & Hall. <https://www.ptonline.com/articles/how-to-get-better-mfi-results>
- Mahesa, K., Sugiantoro, B., & Prayudi, Y. (2019). Pemanfaatan Metode DNA Kriptografi dalam Meningkatkan Keamanan Citra Digital. *Jurnal Ilmiah Informatika (JIF)*, 2615–1049.
- Pan, H., Zhang, Q., Caragea, C., Dragut, E., & Jan, L. (n.d.). *FlowLearn : Evaluating Large Vision-Language Models on Flowchart Understanding*.
- Papilaya, R. M., & Pradana, R. (2024). *PENGAMANAN FILE MARKETING PADA YAYASAN PENDIDIKAN DESAIN INDONESIA MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEB MARKETING FILES SECURITY AT THE INDONESIAN DESIGN EDUCATION FOUNDATION USING WEB-BASED AES-256*. 3(September), 109–117.
- Paul, G., & Maitra, S. (2011). RC 4 Stream Cipher variants And It's Variants. In *Teaching Mathematics and its Applications* (Vol. 29, Issue 3).

<https://doi.org/10.1093/teamat/hrq007>

Ratna, S. (2020). Pengolahan Citra Digital Dan Histogram Dengan Phyton Dan

Text Editor Phycharm. *Technologia: Jurnal Ilmiah*, 11(3), 181.

<https://doi.org/10.31602/tji.v11i3.3294>

Rilo Pambudi, A., Garno, & Purwantoro. (2020). DETEKSI KEASLIAN UANG

KERTAS BERDASARKAN WATERMARK DENGAN PENGOLAHAN

CITRA DIGITAL. *Jurnal Informatika Polinema*, 6(4), 69–74.

Romzi, M., & Kurniawan, B. (2020). Pembelajaran Pemrograman Python Dengan

Pendekatan Logika Algoritma. *JTIM: Jurnal Teknik Informatika Mahakarya*,

03(2), 37–44.

Sinaga, M. C. (2017). Kriptografi dan Python. *Academia*, 157.

[https://www.academia.edu/34788898/Kriptografi\\_dan\\_Python\\_pdf](https://www.academia.edu/34788898/Kriptografi_dan_Python_pdf)

## LAMPIRAN



الجامعة الإسلامية سومطرة الشمالية  
UNIVERSITAS ISLAM SUMATERA UTARA  
FAKULTAS TEKNIK  
**PROGRAM STUDI TEKNIK INFORMATIKA**  
JL. S. M. RAJA TELP. : (061) 7868049 FAX. : (061) 7868049 TELADAN MEDAN KODE POS 20217  
www.ft.uisu.ac.id

---

**BERITA ACARA DAN EVALUASI SARAN PEMBANDING SEMINAR SKRIPSI  
PERIODE II BULAN NOVEMBER SEMESTER A. TA – 2024 / 2025**

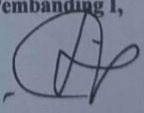
---

Setelah memperhatikan dan mengamati kegiatan seminar Tugas Skripsi yang diadakan pada hari Sabtu tanggal 16 November 2024, waktu 10.00 WIB s/d selesai di Ruang Lab. Komputasi FT. UISU atas Nama Mahasiswa :

|                  |                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------|
| NAMA             | : MAULANA AKBAR                                                                                                   |
| NPM              | : 71220915063                                                                                                     |
| PROGRAM STUDI    | : TEKNIK INFORMATIKA                                                                                              |
| JUDUL SKRIPSI    | : Implementasi Algoritma Advanced Encryption Standard (AES)<br>Untuk Pengamanan Citra Digital                     |
| Dosen Pembimbing | : 1. Mhd. Zulfansyuri Siambaton, ST, M.Kom<br>: 2. Heri Santoso, S.Kom, M.Kom                                     |
| Dosen Pembanding | : 1. Khairuddin Nasution, ST, M.Kom<br>: 2. Rachmat Aulia, S.Kom, M.Sc.IT<br>: 3. Tasliyah Haramaini, S.Si, M.Kom |

Maka oleh karena itu saya sebagai Dosen Pembanding memberikan saran sebagai bahan masukan untuk mahasiswa tersebut di atas dalam menghadapi sidang sarjana adalah sebagai berikut :

1. ✓ Baca Panduan TA : perbaiki kembali kembali
2. ✓ Tingkatkan kembali kriptografi : AES
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_

Medan, 16 November 2024  
Pembanding I,  
  
Khairuddin Nasution, ST, M.Kom



الجامعة الإسلامية في سومطرة الشمالية  
UNIVERSITAS ISLAM SUMATERA UTARA  
FAKULTAS TEKNIK  
**PROGRAM STUDI TEKNIK INFORMATIKA**  
JL. S. M. RAJA TELP. : (061) 7868049 FAX. : (061) 7868049 TELADAN MEDAN KODE POS 20217  
www.ft.uisu.ac.id

**BERITA ACARA DAN EVALUASI SARAN PEMBANDING SEMINAR SKRIPSI  
PERIODE II BULAN NOVEMBER SEMESTER A. TA – 2024 / 2025**

Setelah memperhatikan dan mengamati kegiatan seminar Tugas Skripsi yang diadakan pada hari Sabtu tanggal 16 November 2024, waktu 10.00 WIB s/d selesai di Ruang Lab. Komputasi FT. UISU atas Nama Mahasiswa :

NAMA : MAULANA AKBAR  
NPM : 71220915063  
PROGRAM STUDI : TEKNIK INFORMATIKA  
JUDUL SKRIPSI : Implementasi Algoritma Advanced Encryption Standard (AES)  
Untuk Pengamanan Citra Digital  
Dosen Pembimbing : 1. Mhd. Zulfansyuri Siambaton, ST, M.Kom  
2. Heri Santoso, S.Kom, M.Kom  
Dosen Pembanding : 1. Khairuddin Nasution, ST, M.Kom  
2. Rachmat Aulia, S.Kom, M.Sc.IT  
3. Tasliyah Haramaini, S.Si, M.Kom

Maka oleh karena itu saya sebagai Dosen Pembanding memberikan saran sebagai bahan masukan untuk mahasiswa tersebut di atas dalam menghadapi sidang sarjana adalah sebagai berikut :

1. Berikan info tentang batasan maksimal ukuran gambar yg dapat di enkripsi/dekripsi
2. Pilih salah satu kunci saja dari kunci yg disediakan, karena titik ini perbedaan
3. Kurang fokus. Judul bahas tentang Citra. Sementara contoh kriptografi text. (Sangat)
4. Kesimpulan dan Saran mohon dibuat per point
5. Pahami tentang konsep dasar AES.

Medan, 16 November 2024

Pembanding II,

Rachmat Aulia, S.Kom, M.Sc.IT



الجامعة الإسلامية في سومطرة الشمالية  
UNIVERSITAS ISLAM SUMATERA UTARA  
FAKULTAS TEKNIK  
**PROGRAM STUDI TEKNIK INFORMATIKA**  
JL. S. M. RAJA TELP. : (061) 7868049 FAX. : (061) 7868049 TELADAN MEDAN KODE POS 20217  
www.ft.uisu.ac.id

**BERITA ACARA DAN EVALUASI SARAN PEMBANDING SEMINAR SKRIPSI  
PERIODE II BULAN NOVEMBER SEMESTER A. TA – 2024 / 2025**

Setelah memperhatikan dan mengamati kegiatan seminar Tugas Skripsi yang diadakan pada hari Sabtu tanggal 16 November 2024, waktu 10.00 WIB s/d selesai di Ruang Lab. Komputasi FT. UISU atas Nama Mahasiswa :

NAMA : MAULANA AKBAR  
NPM : 71220915063  
PROGRAM STUDI : TEKNIK INFORMATIKA  
JUDUL SKRIPSI : Implementasi Algoritma Advanced Encryption Standard (AES)  
Untuk Pengamanan Citra Digital  
Dosen Pembimbing : 1. Mhd. Zulfansyuri Siambaton, ST, M.Kom  
: 2. Heri Santoso, S.Kom, M.Kom  
Dosen Pembanding : 1. Khairuddin Nasution, ST, M.Kom  
: 2. Rachmat Aulia, S.Kom, M.Sc.IT  
: 3. Tasliyah Haramaini, S.Si, M.Kom

Maka oleh karena itu saya sebagai Dosen Pembanding memberikan saran sebagai bahan masukan untuk mahasiswa tersebut di atas dalam menghadapi sidang sarjana adalah sebagai berikut :

1. Batasan masalah dgn variasi kunci di perjelas dlm penjelasan teori Bab II
2. t/masukan alasan pemilihan kunci 192 bit
3. Pembahasan membahas 3 kunci & disebut pd. batasan (128, 192, 256),  
dan uji beda & kelebihan pd. 3 kunci tsb.
4. Kesimpulan & saran perlu diperbaiki sesuaikan dgn judul skripsi  
et hasil penelitian

Medan, 16 November 2024

Pembanding III,

Tasliyah Haramaini, S.Si, M.Kom