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 ilmiyah 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

Daftar Tabel

Daftar Gambar

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

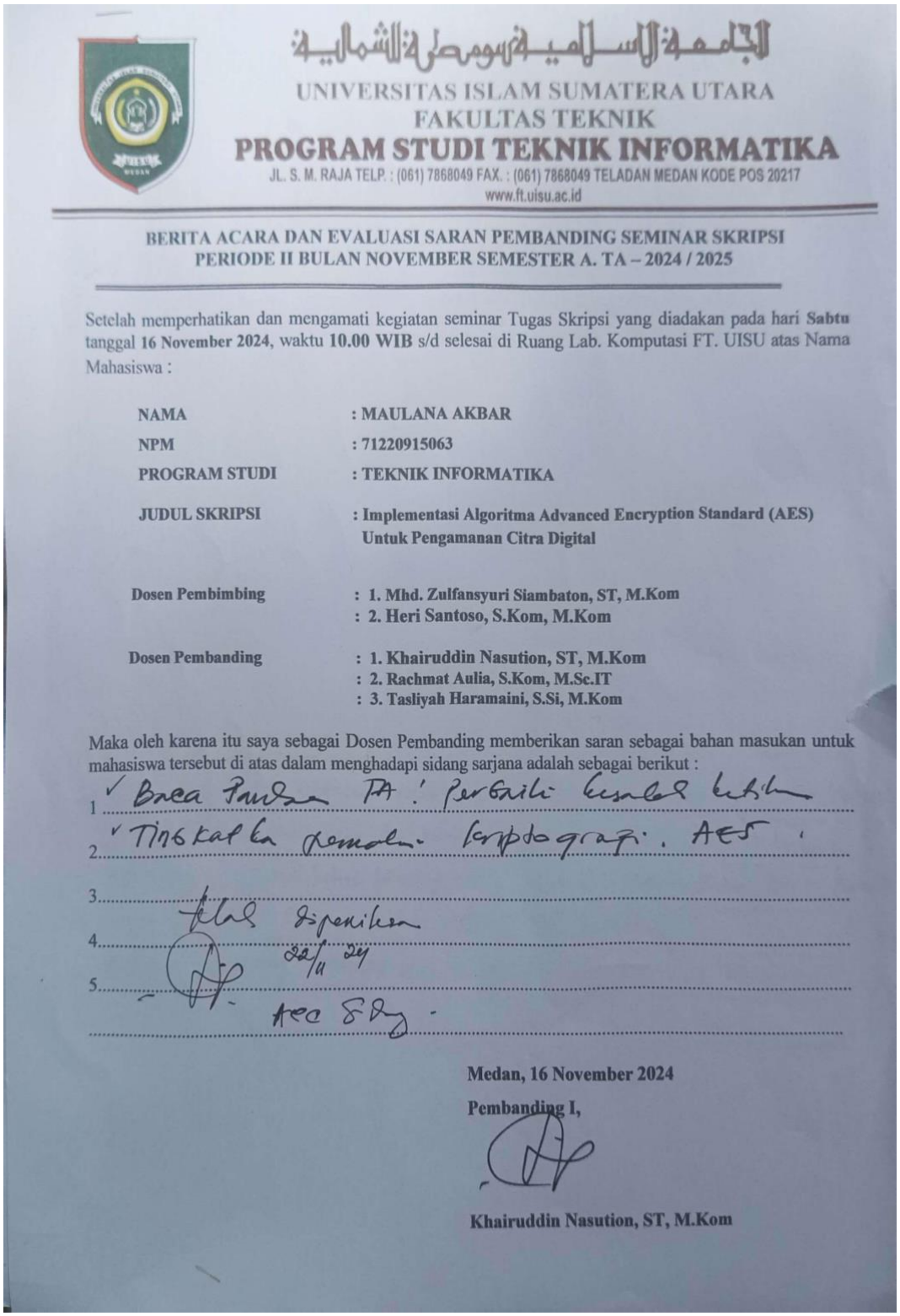
Ratna, S. (2020). Pengolahan Citra Digital Dan Histogram Dengan Phyton Dan Text Editor Phycharm. *Technologia: Jurnal Ilmiah*, *11*(3), 181. https://doi.org/10.31602/tji.v11i3.3294

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

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) 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**

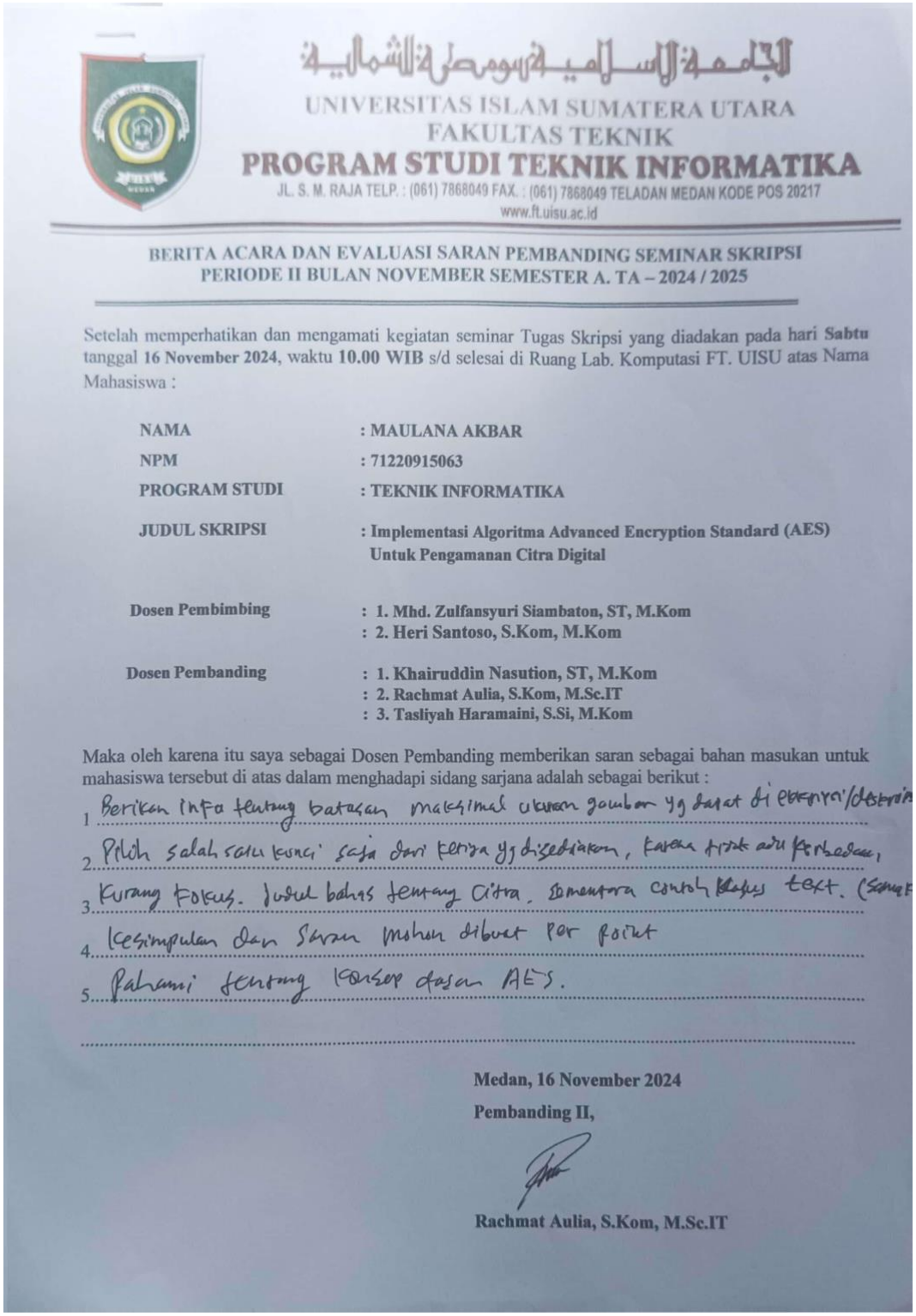
Maka oleh karena itu saya sebagai Dosen Pembanding memberikan saran sebagai bahan masukan untuk mahasiswa tersebut di atas dalam menghadapi sidang sarjana adalah sebagai berikut :

1. ✓ Baca Pandan TA ! Perbaiki kesalah tulisan
2. ✓ Tingkatkan pemahaman kriptografi . AES .
3. Sudah disperiksa
4. 22/11 24
5. Acc Sdg .

Medan, 16 November 2024

Pembanding I,

Khairuddin Nasution, ST, M.Kom



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) 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 ekstraksi/destrip
2. Pilih salah satu kunci saja dari kunci yg disediakan, karena untuk asli berbeda,
3. Kurang fokus. Judul bahas tentang citra, Sementara contoh kasus text. (Semest
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 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 diperjelas dlm penjelasan teori Bab II
2. Utk alasan pemilihan kunci 192 bit
3. Pembahasan membahas 3 kunci yg disebut pd. batasan (128, 192, 256),
4. dan Uji beda & kelebihan pd. 3 kunci tsb.
5. Kesimpulan & saran perlu diperbaiki sesuaikan dgn judul skripsi & hasil penelitian

Medan, 16 November 2024

Pembanding III,

Tasliyah Haramaini, S.Si, M.Kom