

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES
(*ADVANCED ENCRYPTION STANDARD*) RIJNDAEL DALAM
KEAMANAN TEKS CATATAN BERBASIS ANDROID**

SKRIPSI

SITI FATIMAH

0701173206



PROGRAM STUDI ILMU KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUMATERA UTARA

MEDAN

2022

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES
(ADVANCED ENCRYPTION STANDARD) RIJNDAEL DALAM
KEAMANAN TEKS CATATAN BERBASIS ANDROID**

SKRIPSI

Diajukan Untuk Memenuhi Syarat Mencapai Gelar Sarjana Komputer

SITI FATIMAH

0701173206



PROGRAM STUDI ILMU KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUMATERA UTARA

MEDAN

2022

PERSETUJUAN SKRIPSI

Hal : Surat Persetujuan
Lamp :-

Kepada Yth.,
Dekan Fakultas Sains Dan Teknologi
Universitas Islam Negeri Sumatera Utara Medan

Assalamu'alaikum Wr Wb.

Setelah membaca, meneliti, memberikan petunjuk, dan mengoreksi serta mengadakan perbaikan, maka kami selaku pembimbing berpendapat bahwa skripsi saudara

Nama : Siti Fatimah
Nomor Induk Mahasiswa : 0701173206
Program Studi : Ilmu Komputer
Judul Skripsi : Implementasi Algoritma Kriptografi
AES (*Advanced Encryption Standard*)
Rijndael Dalam Keamanan Teks
Catatan Berbasis Android

Dapat disetujui dan segera *dimunqossahkan*, atas perhatiannya kami ucapkan terima kasih

Medan, 02 Februari 2022

21 Rajab 1443 H

Pembimbing Skripsi I

Pembimbing Skripsi II

(Ilka Zufria, M.Kom)
NIP. 198506042015031006

(Yusuf Ramadhan Nasution, M.Kom)
NIB. 1100000075

SURAT PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini:

Nama : Siti Fatimah

Nomor Induk Mahasiswa : 0701173208

Program Studi : Ilmu Komputer

Judul : Implementasi Algoritma Kriptografi AES
(*Advanced Encryption Standard*) Rijndael Dalam
Keamanan Teks Catatan Berbasis Android

Menyatakan bahwa skripsi ini adalah hasil karya saya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya. Apabila di kemudian hari ditemukan plagiat dalam skripsi ini maka saya bersedia menerima sanksi pencabutan gelar akademik yang saya peroleh dan sanksi lainnya sesuai dengan peraturan yang berlaku.

Medan, 14 Februari 2022



Siti Fatimah

NIM.0701173206

UIN
SUMATERA UTARA
MEDAN



**KEMENTERIAN AGAMA REPUBLIK INDONESIA UNIVERSITAS
ISLAM NEGERI SUMATERA UTARA MEDAN FAKULTAS SAINS
DAN TEKNOLOGI**

Jl. IAIN No. 1 Medan 20235

Telp. (061) 6615683-6622925, Fax. (061) 6615683

Url: <http://saintek.uinsu.ac.id>, E-mail: saintek@uinsu.ac.id

PENGESAHAN SKRIPSI

Nomor: B.125/ST/ST.V.2/PP.01.1/06/2022

Judul : Implementasi Algoritma Kriptografi AES (*Advanced Encryption Standard*) Rijndael Dalam Keamanan Teks Catatan Berbasis Android
Nama : Siti Fatimah
Nomor Induk Mahasiswa : 0701173206
Program Studi : Ilmu Komputer
Fakultas : Sains dan Teknologi

Telah dipertahankan di hadapan Dewan Penguji Skripsi Program Studi Ilmu Komputer Fakultas Sains dan Teknologi UIN Sumatera Utara Medan dan dinyatakan **LULUS**.

Pada hari/tanggal : Selasa, 22 Februari 2022
Tempat : Ruang Sidang Fakultas Sains dan Teknologi UIN Sumatera Utara Medan, Kampus IV- Tuntungan

Tim Ujian Munaqasyah,
Ketua,

Ilka Zufria, M.Kom.
NIP. 198506042015031006

Penguji I, Dewan Penguji,
Penguji II,

Heri Santoso, M.Kom.
NIB. 1100000114

Supiyandi, M.Kom.
NIB. 0701209006

Penguji III,

Penguji IV,

Ilka Zufria, M.Kom.
NIP. 198506042015031006

Yusuf Ramadhan Nasution, M.Kom.
NIB. 1100000075

Mengesahkan,
Dekan Fakultas Sains dan Teknologi
UIN Sumatera Utara Medan

Dr. Mhd Syahnan, M.A.
NIP. 196609051991031002

ABSTRAK

Catatan adalah sesuatu kebutuhan untuk notifikasi setiap saat yang sangat penting. Tapi untuk menyimpan data tersebut, membutuhkan sesuatu agar terjaga. Kerahasiaan data catatan tentunya tidak memiliki keinginan untuk diketahui dan diambil oleh orang lain. Oleh karena itu penulis sangat menginginkan suatu kerangka keamanan yang dapat mengikuti data tersebut, khususnya dengan aplikasi catatan yang menggunakan kriptografi. Untuk itulah dalam skripsi dibuat suatu aplikasi teks catatan berbasis android yang dapat mengamankan teks yang ingin di enkripsi. Dengan menggunakan algoritma kriptografi AES (*Advanced Encryption Standard*) Rijndael dengan panjang kunci 128 bit, 192 bit dan 256 bit. Mulai dari judul dan dekripsi tidak terbatas teks yang di input, dan kunci yang terbatas dengan tipe AES yaitu 128 bit, 192 bit, dan 256 bit akan mampu menjaga keamanan data tersebut dengan lebih baik. Di bangun dengan berbasis android akan memudahkan bagi para pengguna dalam mengakses aplikasi tersebut.

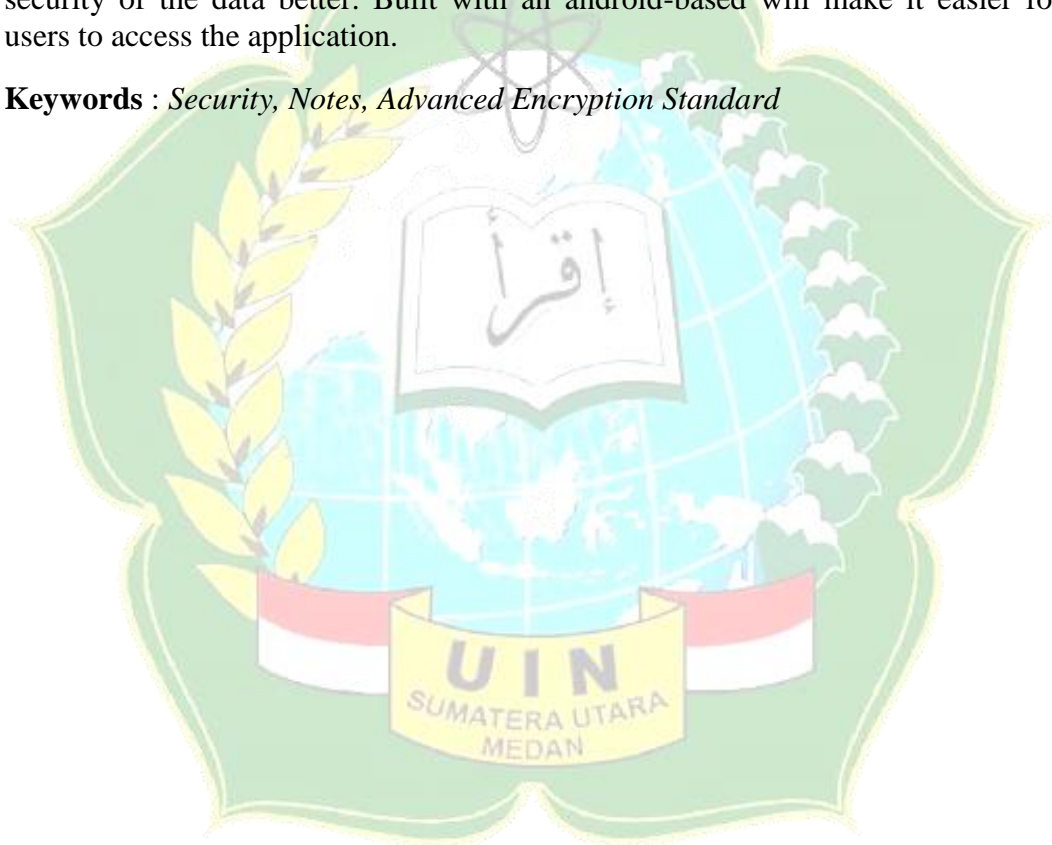
Kata kunci : Keamanan, Catatan, *Advanced Encryption Standard*



ABSTRACT

Notes is something that needs to be notified at any time which is very important. But to store that data, you need something to keep it awake. Confidentiality of record data certainly has no desire to be known and taken by others. Therefore, the author really wants a security framework that can follow the data, especially with note applications that use cryptography. For this reason, in this thesis, an android-based note text application is made that can secure the text you want to encrypt. By using Rijndael's AES (Advanced Encryption Standard) cryptographic algorithm with a key length of 128 bits, 192 bits and 256 bits. Starting from the title and decryption of unlimited text input, and a limited key with AES type of 128 bits, 192 bits, and 256 bits will be able to maintain the security of the data better. Built with an android-based will make it easier for users to access the application.

Keywords : *Security, Notes, Advanced Encryption Standard*



KATA PENGANTAR

Alhamdulillah, puji dan syukur kehadiran Allah SWT, atas segala kenikmatan dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi ini dengan judul “Implementasi Algoritma Kriptografi AES (*Advanced Encryption Standard*) Rijndael Dalam Keamanan Teks Catatan Berbasis Android”. Sebagai salah satu syarat untuk mendapatkan gelar Sarjana Ilmu Komputer, pada Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara. Sholawat serta kabar gembira untuk Nabi Muhammad SAW yang tiada taranya yang luar biasa, yang telah membawa sanak saudaranya dari zaman kegelapan ke zaman cahaya agung yang kita rasakan saat ini. Semoga kita mendapatkan syafaat-Nya di yaumul terakhir nanti. Amin ya Rabbal Alamin.

Pada kesempatan ini, penulis ingin menyampaikan terima kasih yang luar biasa kepada orang tua tersayang yang telah mendidik, membesarkan, memberikan cinta yang tak ternilai, dan yang selalu mendoakan yang terbaik untuk anaknya, yakni ayah saya (Sugiono) dan ibu saya (Nurhayati), yang selalu memberikan dukungan yang penuh untuk dapat menyelesaikan skripsi ini untuk mendapatkan gelar Sarjana Ilmu Komputer, di Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara.

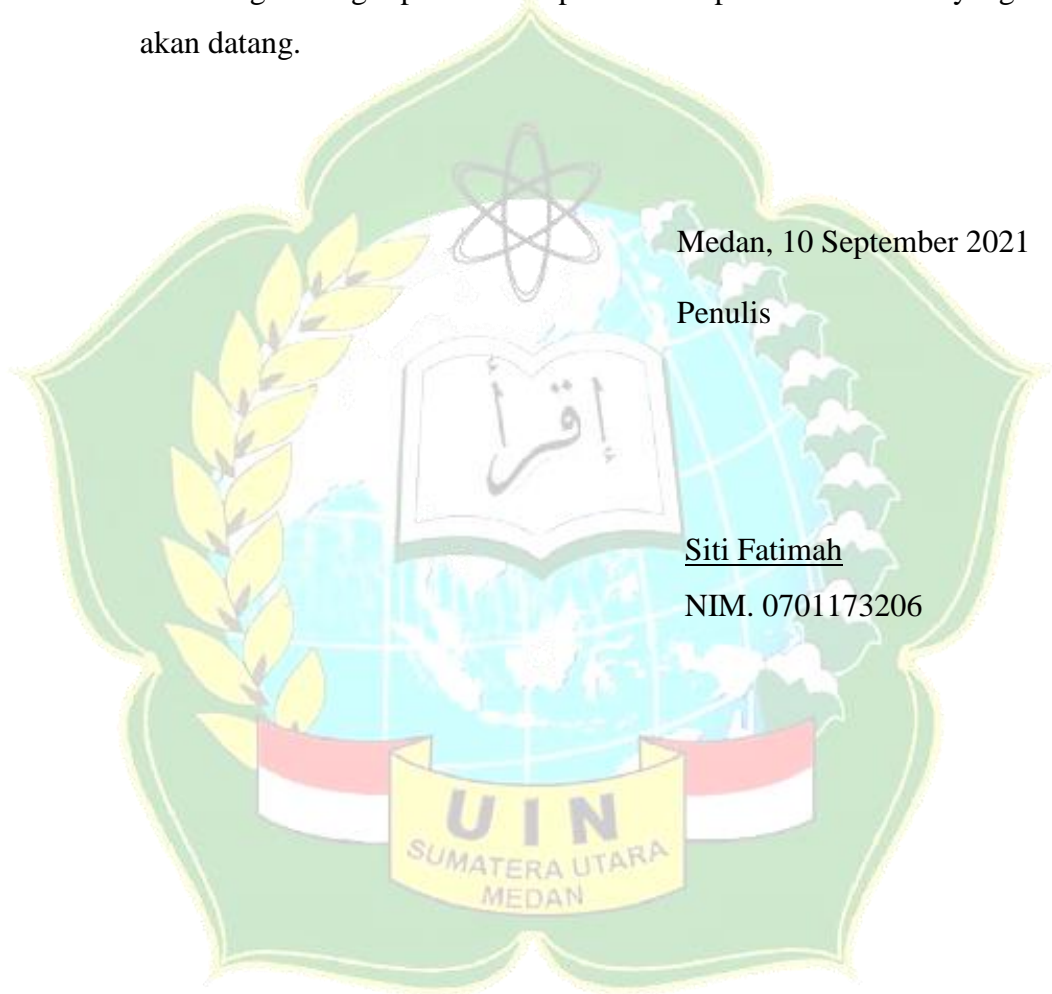
Penulis memahami bahwa dalam penyusunan proposal ini, tidak akan berjalan seperti yang diharapkan tanpa kursus dan arahan serta dorongan dan bantuan dari berbagai pihak, oleh karena itu dengan segala kerendahan hati penulis ingin mengucapkan terima kasih kepada:

Bapak Prof. Dr. Syahrin Harahap, MA, selaku Rektor Universitas Islam Negeri Sumatera Utara.

1. Bapak Dr. Mhd. Syahnan, M.A, selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.
2. Bapak Ilka Zufria, M.Kom, selaku Ketua Prodi Ilmu Komputer Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.
3. Bapak Rakhmat Kurniawan, M.Kom, selaku Sekertaris Prodi Ilmu Komputer Fakultas Sains dan Tekonologi Universitas Islam Negeri Sumatera Utara.
4. Bapak Heri Santoso, M.Kom, selaku Dosen Pembimbing Akademik dari mulai penulis menjadi mahasiswa baru sampai semester VII di Universitas Islam Negeri Sumatera Utara, yang selalu memotivasi penulis agar selalu bersungguh-sungguh di dalam mengikuti perkuliahan di Universitas Islam Negeri Sumatera Utara.
5. Bapak Ilka Zufria, M.Kom, selaku Dosen Pembimbing Skripsi I, yang senantiasa memberikan arahan dan masukan kepada peneliti dalam penyelesaian skripsi ini.
6. Bapak Yusuf Ramadhan Nasution, M.Kom, selaku Dosen Pembimbing Skripsi II yang selalu memberikan bantuan, nasehat, arahan, bimbingan dalam penyelesaian skripsi ini.
7. Seluruh Dosen dan Pegawai Prodi Ilmu Komputer di Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara.
8. Teman Seperjuang Skripsi, Rohima Amalia Siregar, Siti Nurhaliza Sofyan, Sulistiani, Fuji Rahayu S, dan Syahdinda Octaviana Yang tidak kenal lelah dan menyerah dalam mengerjakan skripsi.
9. Teman Seperjuangan Ilmu Komputer 6, yang selama ini bersama-sama mengikuti perkuliahan dalam satu kelas di Prodi Ilmu Komputer Universitas Islam Negeri Sumatera Utara.

10. Teman Seperjuangan Ilmu Komputer Stambuk 2017, yang selama ini bersama-sama mengikuti perkuliahan di Prodi Ilmu Komputer di Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.

Penulis berharap semoga skripsi ini dapat bermanfaat dan menambah wawasan keilmuan. Kritik dan saran yang sifatnya membangun sangat penulis harapkan untuk perbaikan dimasa yang akan datang.



Medan, 10 September 2021

Penulis

Siti Fatimah

NIM. 0701173206

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR.....	iii
DAFTAR ISI.....	vi
DAFTAR TABEL	ix
DAFTAR GAMBAR.....	x
DAFTAR LAMPIRAN	xii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2.Rumusan Masalah.....	4
1.3.Batasan Masalah	4
1.4.Tujuan Penelitian	5
1.5.Manfaat Penelitian	5
BAB II TINJAUAN PUSTAKA.....	6
2.1 Kriptografi	6
2.1.1 Kriptografi Simetris.....	7
2.1.2 Kriptografi Asimetris	8
2.2 Advanced Encryption Standard	8
2.3 Rijndael.....	9
2.3.1 Enkripsi	10
2.3.1.1 Transformasi SubBytes	11
2.3.1.2 Transformasi ShiftRows	12
2.3.1.3 Transformasi MixColumns.....	12
2.3.1.4 Transformasi AddRoundKey.....	13
2.3.1.5 Ekspansi Kunci (<i>Key Schedule</i>).....	14
2.3.2 Dekripsi	16

2.4 ECB (<i>Electronic Code Book</i>)	17
2.5 Andorid	18
2.5.1 Sejarah Android.....	19
2.5.2 Komponen Android.....	19
2.5.3 Arsitektur Android	20
2.5.4 Versi Android.....	22
2.6 Android Studio	24
2.7 SQLite.....	24
2.8 Java	25
2.9 Flowchart (Bagan Alir).....	25
2.10 Penelitian Terdahulu.....	27
BAB III METODE PENELITIAN	31
3.1 Waktu dan Jadwal Pelaksanaan Penelitian	31
3.2 Alat dan Bahan Penelitian	31
3.2.1 Bahan Penelitian	32
3.2.2 Alat Penelitian	32
3.3 Cara Kerja.....	32
3.3.1 Metode Pengembangan Sistem.....	33
3.3.2 Teknik Pengumpulan Data	33
3.3.3 Analisis Kebutuhan	34
3.3.3.1 Metode Analisis.....	35
3.3.3.2 Hasil Analisis.....	38
3.3.4 Perancangan.....	39
3.3.5 Pengujian	39
3.3.6 Penerapan.....	39
BAB IV HASIL DAN PEMBAHASAN	40
4.1 Pembahasan	40
4.1.1 Analisis Data	40
4.1.2 Representasi Data	41
4.1.3 Perancangan.....	50
4.1.3.1 Perancangan Interface (Antarmuka).....	50

4.1.3.2 Flowchart Sistem	54
4.2 Hasil	55
4.2.1 Implementasi Sistem	55
4.2.2 Pengujian	58
4.2.3 Penerapan.....	62
BAB V KESIMPULAN DAN SARAN	63
5.1 Kesimpulan.....	63
5.2 Saran.....	63
DAFTAR PUSTAKA	64
LAMPIRAN	



DAFTAR TABEL

Tabel	Judul Tabel	Halaman
2.1	Jumlah Putaran AES Rijndael.....	9
2.2	Tabel <i>S-Box</i>	12
2.3	Tabel Flowchart.....	26
2.4	Daftar Penelitian Terdahulu.....	27
3.1	Jadwal Penelitian.....	31
4.1	Rcon.....	42
4.2	Inverse S-Box.....	42
4.3	Chipher key.....	42
4.4	Proses Rotword, S-Box, dan Rcon.....	43
4.5	Cara mencari tabel S-Box.....	44
4.6	Proses ShiftRows.....	44
4.7	Output ShiftRows.....	44
4.8	Matriks GF (8).....	45
4.9	Rancangan Halaman Utama.....	51
4.10	Rancangan halaman Proses.....	52
4.11	Rancangan halaman Output.....	53

DAFTAR GAMBAR

Gambar	Judul Gambar	Halaman
2.1	Algoritma Enkripsi AES Rijndael.....	10
2.2	Transformasi <i>ShiftRows</i>	12
2.3	Transformasi <i>MixColumns</i>	13
2.4	Transformasi <i>AddRoundKey</i>	13
2.5	Hasil <i>AddRoundKey</i>	13
2.6	Proses mencari round key-1	14
2.7	Perhitungan XOR antar kolom pertama key	14
2.8	Perhitungan XOR antar kolom kedua key	15
2.9	Perhitungan XOR antar kolom ketiga key	15
2.10	Proses <i>Key Schedule</i>	16
2.11	Hasil Enkripsi.....	16
2.12	Diagram Alur Proses Dekripsi AES.....	17
2.13	ECB (<i>Electronic Code Book</i>) mode enkripsi	18
2.14	ECB (<i>Electronic Code Book</i>) mode dekripsi	18
2.15	Arsitektur Android	22
3.1	Proses Tahapan Perancangan	33
3.2	<i>Flowchart</i> Algoritma Enkripsi AES	35
3.3	<i>Flowchart</i> Algoritma Dekripsi AES	37
4.1	Rancangan halaman utama	50
4.2	Rancangan halaman Proses.....	51
4.3	Rancangan halaman Output	53
4.4	<i>Flowchart enkripsi</i> sistem.....	54
4.5	<i>Flowchart dekripsi</i> sistem.....	55
4.6	Halaman Utama	56
4.7	Halaman Proses.....	57
4.8	Halaman Update.....	57

4.9	Halaman Input Plaintext 128 bit.....	58
4.10	Halaman Output Chipertext 128 bit.....	59
4.11	Halaman Input Plaintext 192 bit.....	59
4.12	Halaman Output Chipertext 192 bit.....	59
4.13	Halaman Input Plaintext 256 bit.....	60
4.14	Halaman Output Chipertext 256 bit.....	61
4.11	Notifikasi pada enkripsi.....	61
4.12	Notifikasi pada dekripsi.....	62



DAFTAR LAMPIRAN

Lampiran	Judul Lampiran
1.	Listing Program <i>AES (Advanced Encryption Standard)</i> Rijndael
2.	Tabel Pengujian black-box
3.	Kode ASCII
4.	Daftar Riwayat Hidup
5.	Kartu Bimbingan Skripsi

