

**IMPLEMENTASI ALGORITMA AES PADA
APLIKASI ARSIP SURAT DI DIREKTORAT
PENGEMBANGAN TEKNOLOGI
INFORMASI UBHARA JAYA**

SKRIPSI

Oleh:

Alifudin Alfarizi

201810225010



**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BHAYANGKARA JAKARTA RAYA
2022**

LEMBAR PERSETUJUAN PEMBIMBING

LEMBAR PERSETUJUAN PEMBIMBING

Judul Skripsi : Implementasi Algoritma AES pada Aplikasi Arsip
Surat di Direktorat Pengembangan Teknologi
Informasi Ubhara Jaya

Nama Mahasiswa : Alifudin Alfarizi
Nomor Pokok Mahasiswa : 201810225010
Program Studi/Fakultas : Informatika / Ilmu Komputer



LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Judul Proposal Skripsi : Implementasi Algoritma AES pada Aplikasi
Arsip Surat di Direktorat Pengembangan Teknologi
Informasi Ubhara Jaya

Nama Mahasiswa : Alifudin Alfari

Nomor Pokok Mahasiswa : 201810225010

Program Studi/Fakultas : Informatika / Ilmu Komputer

Tanggal Lulus Ujian Skripsi : 25 Juli 2022

Bekasi, 29 Juli 2022

MENGESAHKAN

Ketua Tim Penguji : Achmad Noe'man, S.Kom., M.Kom.

NIDN : 0328048402

Penguji I : Dr. Tb. Ai Munandar, S.Kom., MT.

NIDN : 0413098403

Penguji II : Sugiyatno, S.Kom., M.Kom.

NIDN : 0313077206

MENGETAHUI,

Ketua Prodi
Informatika

Dekan
Fakultas Ilmu Komputer

Ahmad Fathurrozi, S.E., M.M.S.I.

NIP. 2012486

Dr. Dra. Tyastuti Sri Lestari, M.M.

NIP. 1408206

LEMBAR PERNYATAAN BUKAN PLAGIASI



UNIVERSITAS BHAYANGKARA JAKARTA RAYA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA

LEMBAR PERNYATAAN BUKAN PLAGIASI

Yang bertanda tangan dibawah ini :

Nama : Alifudin Alfarizi
NPM : 201810225010
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul Tugas Akhir : Implementasi Algoritma AES pada Aplikasi Arsip Surat di
Direktorat Pengembangan Teknologi Informasi Ubhara Jaya

Dengan ini menyatakan bahwa hasil penulisan skripsi yang telah saya buat ini merupakan **hasil karya saya sendiri dan benar keasliannya**. Apabila dikemudian hari penulisan skripsi ini merupakan plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggungjawabkan sekaligus bersedia menerima sanksi berdasarkan tata tertib di Universitas Bhayangkara Jakarta Raya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan dari pihak manapun.

Bekasi, 05 Agustus 2022

Penulis



Alifudin Alfarizi

ABSTRAK

Alifudin Alfarizi. 201810225010. “Implementasi Algoritma AES pada Aplikasi Arsip Surat di Direktorat Pengembangan Teknologi Informasi Ubhara Jaya”.

Kegiatan pengarsipan manual yang dilakukan setiap hari dan terkadang sulit untuk menemukan kembali dokumen yang sudah diarsipkan membuat Direktorat Pengembangan Teknologi Informasi Ubhara Jaya (Dit. PTI UBJ) menciptakan sebuah Aplikasi Arsip Surat. Aplikasi tersebut memudahkan Dit. PTI dalam pendataan, pengarsipan, serta pencarian dokumen surat yang sudah diarsipkan, hanya saja saat ini belum diterapkan metode apapun dalam pengamanan file arsip suratnya. Penelitian ini menitikberatkan pada pengembangan aplikasi arsip surat yang sudah berjalan dengan mengimplementasikan algoritma AES-256 pada pengamanan file arsip surat. Advanced Encryption Standard (AES) merupakan algoritma cryptographic yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blokchipertext simetrik yang dapat mengenkripsi dan dekripsi informasi. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits. Supaya algoritma AES-256 dapat diimplementasikan pada sistem yang sedang berjalan, digunakanlah bantuan library native dari bahasa pemrograman go, yaitu crypto/cipher dan crypto/aes agar dapat diterapkannya proses enkripsi dan dekripsi terhadap file arsip surat yang akan diarsipkan kedalam aplikasi. Dengan dilakukannya pengembangan sistem pada aplikasi arsip surat yang saat ini sedang berjalan dapat memberikan rasa percaya dan aman kepada pengguna serta menghasilkan sistem pengarsipan yang lebih aman dari sebelumnya.

Kata kunci: Algoritma AES, Arsip Surat, Aplikasi Arsip Surat, E-Arsip, Ubhara Jaya, Enkripsi dan Dekripsi

ABSTRACT

Alifudin Alfarizi. 201810225010. “Implementation of the AES Algorithm in the Mail Archive Application at the Directorate of Information Technology Development of Ubhara Jaya”.

Manual archiving activities that are carried out every day and sometimes it is difficult to find back archived documents make the Directorate of Information Technology Development of Ubhara Jaya (Directorate. PTI UBJ) create a Letter Archive Application. The application makes it easier for Directorate. PTI in data collection, archiving, and searching for archived mail documents, it's just that at this time no method has been applied in securing the archived mail files. This research focuses on the development of a mail archive application that is already running by implementing the AES-256 algorithm for securing mail archive files. Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used to secure data. The AES algorithm is a symmetric ciphertext block that can encrypt and decrypt information. The AES algorithm uses a cryptographic key of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. So that the AES-256 algorithm can be implemented on a running system, native libraries from the go programming language are used, namely crypto/cipher and crypto /aes so that the encryption and decryption process can be applied to the letter archive files that will be archived into the application. By developing a system on the mail archive application that is currently running, it can provide a sense of trust and security to users and produce an archiving system that is safer than before.

Keywords: AES Algorithm, Mail Archive, Mail Archive Application, E-Archive, Ubhara Jaya, Encryption and Decryption

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

Sebagai sivitas akademik Universitas Bhayangkara Jakarta Raya, saya yang bertanda tangan di bawah ini :

Nama : Alifudin Alfarizi
NPM : 201810225010
Program Studi : Informatika
Fakultas : Ilmu Komputer
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bhayangkara Jakarta Raya **Hak Bebas Royalti Non-Eksklusif (Non-Exclusive Royalty-Free Right)**, atas karya ilmiah saya yang berjudul :

Implementasi Algoritma AES pada Aplikasi Arsip Surat di Direktorat Pengembangan Teknologi Informasi Ubhara Jaya

berserta perangkat yang ada (bila diperlukan). Dengan hak bebas royalti non-eksklusif ini, Universitas Bhayangkara Jakarta Raya berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya dan mempublikasikannya di Internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik hak cipta.

Segala bentuk tuntutan hukum yang timbul atas pelanggaran hak cipta dalam karya ilmiah ini menjadi tanggung jawab saya pribadi

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Bekasi
Pada tanggal : 05 Agustus 2022
Yang Menyatakan



Alifudin Alfarizi

KATA PENGANTAR

Alhamdulillahirabbil'alam, segala puji bagi Allah *subhanahu wa ta'ala* Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan hidayah-Nya, karena hanya dengan izin-Nya lah kita dapat melakukan segala aktivitas. Khususnya karena izin-Nya lah penulis dapat menyelesaikan penyusunan dan penulisan skripsi ini tepat pada waktunya.

Penulisan skripsi ini merupakan bagian dari tugas mahasiswa sebagai syarat kelulusan yang telah ditentukan untuk menyelesaikan jenjang studi Strata-1 Informatika di Universitas Bhayangkara Jakarta Raya. Dengan selesainya penulisan skripsi ini, penulis menyampaikan terima kasih kepada kedua orang tua tercinta beserta saudara-saudara penulis yang telah memberikan kesempatan untuk menikmati jenjang kuliah serta selalu mendoakan dan memberika dukungan kepada penulis, tidak lupa juga penulis menyampaikan terima kasih kepada:

1. Bapak Irjen Pol (Purn) Dr. Drs. H. Bambang Karsono, S.H., M.M. Selaku Rektor Universitas Bhayangkara Jakarta Raya.
2. Ibu Dr. Dra. Tyastuti Sri Lestari, M.M. Selaku Dekan Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
3. Bapak Ahmad Fathurrozi, S.E., M.M.S.I. Selaku Ketua Program Studi Informatika Universitas Bhayangkara Jakarta Raya.
4. Bapak Sugiyatno, S.Kom., M.Kom. Selaku dosen pembimbing skripsi satu dan Bapak Prio Kustanto, S.T., M.Kom. Selaku dosen pembimbing skripsi kedua yang telah memberikan arahan serta bimbingan kepada penulis selama jalannya penelitian.
5. Pak Turino, Mas Tri, Mas Tyo, Mba Lia dan Mba Nur serta seluruh karyawan Direktorat Pengembangan Teknologi Universitas Bhayangkara Jakarta Raya yang telah membimbing dan memberikan ilmunya kepada penulis.

Semoga Allah *subhanahu wa ta'ala* memberikan balasan kebaikan yang lebih besar kepada beliau – beliau dan pada akhirnya penulis berharap agar laporan skripsi ini dapat bermanfaat. Demi kesempurnaan penulisan skripsi ini,

penulis selalu mengharapkan adanya saran dan masukan dari berbagai pihak, karena penulis menyadari penulisan skripsi yang telah penulis buat ini masih jauh dari kata sempurna. Harapan penulis semoga penelitian ini dapat memberikan manfaat khususnya bagi penulis sendiri dan umumnya bagi semua pihak yang membacanya.



DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERSETUJUAN PEMBIMBING	ii
LEMBAR PERNYATAAN BUKAN PLAGIASI	iii
ABSTRAK	iv
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
DAFTAR LAMPIRAN	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah.....	4
1.3 Rumusan Masalah.....	4
1.4 Batasan Masalah.....	4
1.5 Tujuan dan Manfaat Penelitian	5
1.6 Sistematika Penulisan	5
BAB II LANDASAN TEORI	7
2.1 Tinjauan Pustaka.....	7
2.2 Pengarsipan.....	8
2.2.1 Arsip	9
2.2.1.1 Perbedaan Arsip dan Kearsipan	9

2.2.1.2	Fungsi Arsip	9
2.2.1.3	Jenis Arsip	9
2.2.1.4	Rentang Waktu Pengelolaan Arsip di Perguruan Tinggi ..	10
2.2.1.5	Pemeliharaan Arsip	10
2.2.1.6	Tujuan dari Pengelolaan Kearsipan Secara Umum	11
2.2.1.7	Langkah Kegiatan Pengelolaan Arsip	11
2.2.2	Arsip Digital.....	12
2.2.2.1	Pengelolaan dan Penyimpanan Arsip Digital.....	12
2.2.2.2	Tujuan Arsip Digital.....	13
2.2.2.3	Media Penyimpanan Komputer	13
2.2.2.4	Contoh Arsip	14
2.2.2.5	Scanning Dalam Penyimpanan Arsip Elektronik.....	14
2.2.2.6	Karakteristik Arsip Digital.....	15
2.2.2.7	Kelebihan dan Kekurangan Arsip Manual	15
2.2.2.8	Kelebihan dan Kekurangan Arsip Digital.....	15
2.2.2.9	Aplikasi Arteri.....	17
2.2.3	Klasifikasi Arsip Ubhara Jaya.....	17
2.3	Kriptografi	21
2.4	Enkripsi dan Dekripsi	21
2.5	Advanced Encryption Standard (AES).....	22
2.5.1	Proses Enkripsi Algoritma AES (Advanced Encryption Standard)	23
2.5.2	Proses Dekripsi Algoritma AES (Advanced Encryption Standard)	24
2.5.3	Perbandingan Algoritma AES (Advanced Encryption Standard)	25
2.6	Go	27

2.7	<i>JavaScript dan ReactJS</i>	27
2.8	<i>Database</i>	27
2.9	<i>PostgreSQL</i>	27
BAB III METODOLOGI PENELITIAN		28
3.1	Tempat dan Waktu Pelaksanaan	28
3.2	Kerangka Penelitian	28
3.3	Metode Pengumpulan Data	29
3.3.1	Studi Pustaka	29
3.3.2	Observasi	29
3.4	Analisa Kebutuhan Sistem	29
3.4.1	Kebutuhan Perangkat Keras	29
3.4.2	Kebutuhan Perangkat Lunak	30
3.5	Analisa Sistem	30
3.5.1	Analisis Sistem	30
3.5.1.1	Analisis Sistem Berjalan	30
3.5.1.2	Analisa Masalah	34
3.5.1.3	Sistem Usulan	35
3.5.1.4	Analisa Kebutuhan Pengguna	38
BAB IV PERANCANGAN SISTEM DAN IMPLEMENTASI		39
4.1	Umum	39
4.2	Pengembangan Sistem Usulan	39
4.2.1	<i>Use Case Diagram</i>	39
4.2.2	<i>Activity Diagram</i>	41
4.2.3	<i>Sequence Diagram</i>	53
4.2.4	<i>Class Diagram</i>	60
4.2.5	Pengembangan Basis Data	61

4.3	Implementasi.....	64
4.3.1	Implementasi Algoritma AES-256 (<i>Adavanced Encryption Standard</i>)	64
4.3.2	Implementasi Antarmuka	68
4.3.2.1	Implementasi Halaman Login	68
4.3.2.2	Implementasi Halaman Arsip Surat Masuk	69
4.3.2.3	Implementasi Halaman Arsip Surat Keluar	72
4.4	Pengujian <i>Blackbox</i>	74
4.5	Pengujian Algoritma AES-256 (<i>Advanced Encryption Standard</i>).....	78
4.6	Perbandingan Ukuran <i>File</i> Sebelum dan Sesudah Enkripsi.....	78
BAB V	PENUTUP.....	82
5.1	Kesimpulan	82
5.2	Saran.....	82
DAFTAR PUSTAKA		84
LAMPIRAN		87

DAFTAR TABEL

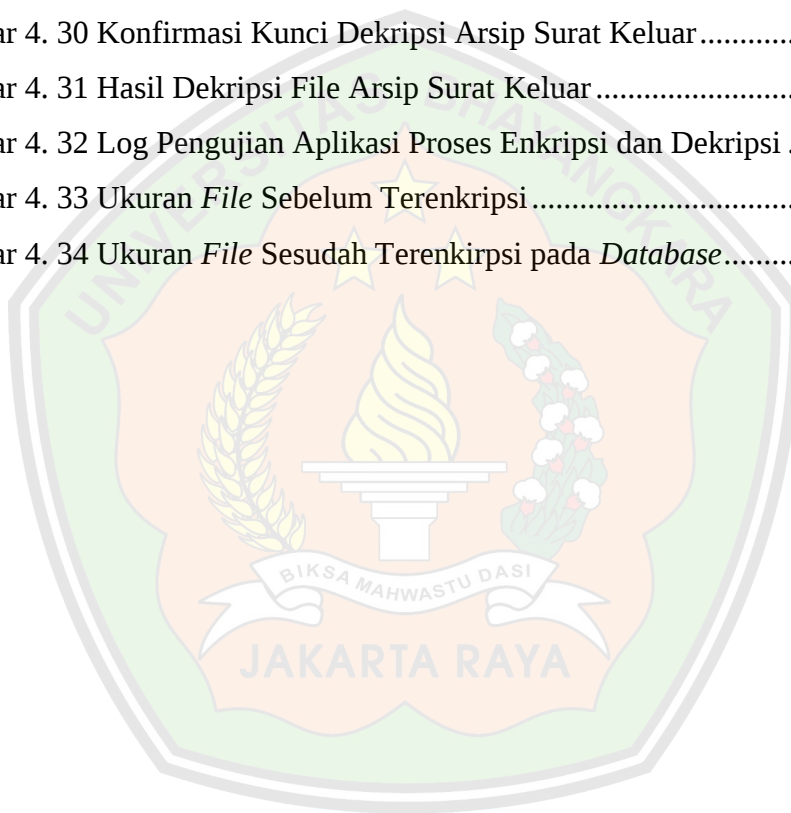
Tabel 2. 1 Penelitian Terkait	7
Tabel 2. 2 Perbandingan Jumlah <i>Key</i> dan <i>Round</i>	22
Tabel 4. 1 <i>Database</i> Tabel Surat.....	61
Tabel 4. 2 <i>Database</i> Tabel Pengguna	62
Tabel 4. 3 <i>Database</i> Tabel Penerima	62
Tabel 4. 4 <i>Database</i> Tabel Auth	63
Tabel 4. 5 <i>Database</i> Tabel Posisi.....	63
Tabel 4. 6 <i>Database</i> Tabel Unit.....	63
Tabel 4. 7 <i>Database</i> Tabel Jenis Surat.....	64
Tabel 4. 8 <i>Database</i> Tabel Status	64
Tabel 4. 9 Tabel Pengujian <i>Blackbox</i>	74
Tabel 4. 10 Ukuran <i>File</i> Sebelum Terenkripsi.....	79
Tabel 4. 11 Ukuran <i>File</i> Sesudah Terenkripsi	80



DAFTAR GAMBAR

Gambar 2. 1 Proses <i>Input Bytes</i> , <i>State Array</i> , dan <i>Output Bytes</i>	23
Gambar 2. 2 Proses Enkripsi Algoritma AES (<i>Advanced Encryption Standard</i>). 24	
Gambar 2. 3 Proses Dekripsi Algoritma AES (<i>Advanced Encryption Standard</i>). 25	
Gambar 2. 4 Perbandingan Waktu Enkripsi dalam <i>Miliseconds</i>	26
Gambar 2. 5 Perbandingan Waktu Dekripsi dalam <i>Miliseconds</i>	26
Gambar 3. 1 <i>Flowmap</i> Sistem Berjalan (Tambah Arsip Surat Masuk atau Keluar)	31
Gambar 3. 2 <i>Flowmap</i> Sistem Berjalan (Buka Arsip Surat Masuk atau Keluar) .	33
Gambar 3. 3 <i>Flowmap</i> Usulan (Tambah Arsip Surat Masuk atau Keluar).....	35
Gambar 3. 4 <i>Flowmap</i> Usulan (Buka File)	37
Gambar 4. 1 <i>Use Case Diagram</i> Sistem Usulan	40
Gambar 4. 2 <i>Activity Diagram</i> Login	41
Gambar 4. 3 <i>Activity Diagram</i> List atau Daftar Arsip Surat Masuk atau Keluar..	42
Gambar 4. 4 <i>Activity Diagram</i> Tambah Arsip Surat Masuk atau Keluar	44
Gambar 4. 5 <i>Activity Diagram</i> Ubah Arsip Surat Masuk atau Keluar	46
Gambar 4. 6 <i>Activity Diagram</i> Hapus Arsip Surat Masuk atau Keluar	48
Gambar 4. 7 <i>Activity Diagram</i> Buka File Arsip Surat Masuk atau Keluar.....	50
Gambar 4. 8 <i>Activity Diagram</i> Logout	52
Gambar 4. 9 <i>Sequence Diagram</i> Login	53
Gambar 4. 10 <i>Sequence Diagram</i> Tambah Arsip Surat Masuk atau Keluar	54
Gambar 4. 11 <i>Sequence Diagram</i> Ubah Arsip Surat Masuk atau Keluar	55
Gambar 4. 12 <i>Sequence Diagram</i> Hapus Arsip Surat Masuk atau Keluar	56
Gambar 4. 13 <i>Sequence Diagram</i> Buka File Arsip Surat Masuk atau Keluar.....	57
Gambar 4. 14 <i>Sequence Diagram</i> Logout	59
Gambar 4. 15 <i>Class Diagram</i> Sistem Usulan	60
Gambar 4. 16 Rancangan <i>Database</i> Sistem Usulan.....	61
Gambar 4. 17 Potongan Kode Enkripsi AES (<i>Adadvanced Encryption Standard</i>)	65
Gambar 4. 18 Potongan Kode Dekripsi AES (<i>Adadvanced Encryption Standard</i>)	66
Gambar 4. 19 Potongan Kode Penggunaan Fungsi Enkripsi	67
Gambar 4. 20 Potongan Kode Penggunaan Fungsi Dekripsi	68

Gambar 4. 21 Halaman <i>Login</i>	69
Gambar 4. 22 Halaman Arsip Surat Masuk	69
Gambar 4. 23 Implementasi Tambah Surat Masuk dengan Kunci Enkripsi.....	70
Gambar 4. 24 Hasil Enkripsi File Arsip Surat Masuk	70
Gambar 4. 25 Konfirmasi Kunci Dekripsi Arsip Surat Masuk.....	71
Gambar 4. 26 Hasil Dekripsi File Arsip Surat Masuk	71
Gambar 4. 27 Halaman Arsip Surat Keluar	72
Gambar 4. 28 Implementasi Tambah Surat Keluar dengan Kunci Enkripsi.....	72
Gambar 4. 29 Hasil Enkripsi File Arsip Surat Keluar	73
Gambar 4. 30 Konfirmasi Kunci Dekripsi Arsip Surat Keluar.....	73
Gambar 4. 31 Hasil Dekripsi File Arsip Surat Keluar	74
Gambar 4. 32 Log Pengujian Aplikasi Proses Enkripsi dan Dekripsi	78
Gambar 4. 33 Ukuran <i>File</i> Sebelum Terenkripsi	79
Gambar 4. 34 Ukuran <i>File</i> Sesudah Terenkripsi pada <i>Database</i>	80



DAFTAR LAMPIRAN

Lampiran 1 Plagiarisme	87
Lampiran 2 Biodata Mahasiswa.....	88
Lampiran 3 Kartu Bimbingan Skripsi.....	89
Lampiran 4 Surat Keterangan Izin Penelitian	91
Lampiran 5 Surat Rekomendasi Dari Pembimbing	92

