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

SKRIPSI

Oleh:

Alifudin Alfarizi

201810225010

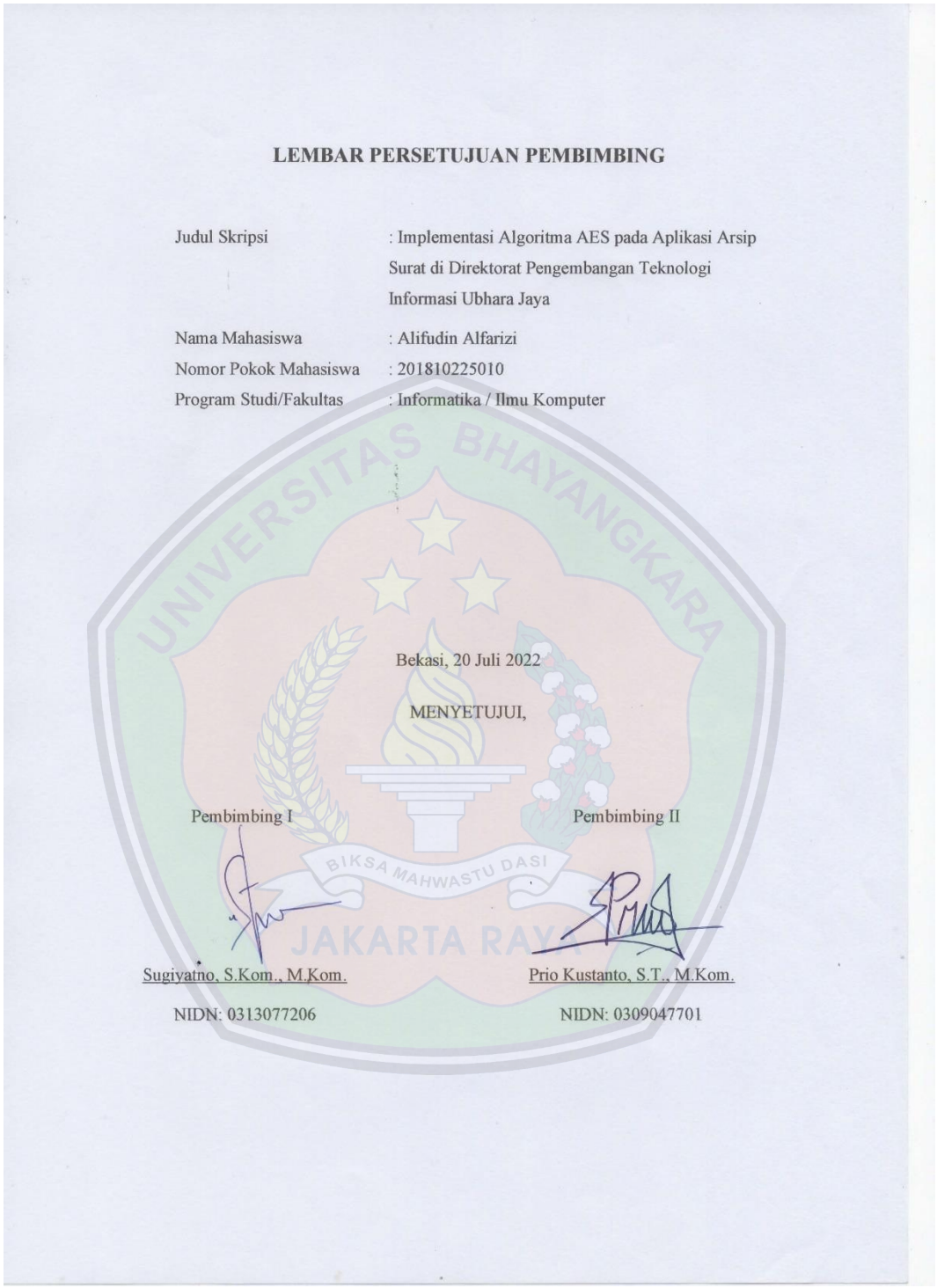
PROGRAM STUDI INFORMATIKA

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

Bekasi, 20 Juli 2022

MENYETUJUI,

Pembimbing I	Pembimbing II
Sugiyatno, S.Kom., M.Kom.	Prio Kustanto, S.T., M.Kom.
NIDN: 0313077206	NIDN: 0309047701

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Judul Proposal 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
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	Dekan
Informatika	Fakultas Ilmu Komputer
Ahmad Fathurrozi, S.E., M.M.S.I.	Dr. Dra. Tyastuti Sri Lestari, M.M.
NIP. 2012486	NIP. 1408206

i

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 digunkan untuk mengamakan data. Algoritma AES adalah blokchipertext simetrik yang dapat mengenkripsi dan dekripsi informasi. Algoritma AES mengunakan 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-Esklusif (*Non-Exclusive Royalty-Free Right*)**, atas karya ilmiah saya yang berjudul :

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

beserta perangkat yang ada (bila diperlukan). Dengan hak bebas royalti non-ekslusif 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'alamin, 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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN