

**PENERAPAN ALGORITMA *ADVANCED ENCRYPTION*  
*STANDARD* (AES-256) DENGAN MODE CBC DAN  
*SECURE HASH ALGORITHM* (SHA-256) UNTUK  
PENGAMANAN DATA FILE**

**SKRIPSI**

**Oleh :**

**SELVIYANI**

**201710225097**



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

**2021**

## LEMBAR PERSETUJUAN PEMBIMBING

Judul Skripsi : Penerapan Algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC dan *Secure Hash Algorithm* (SHA-256) Untuk Pengamanan Data File

Nama Mahasiswa : Selviyani

Nomor Pokok Mahasiswa : 201710225097

Program Studi / Fakultas : Informatika / Ilmu Komputer

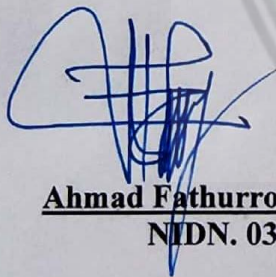
Tanggal Lulus Ujian Skripsi : 14 Juli 2021

Bekasi, 19 Juli 2021

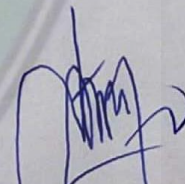
MENYETUJUI,

Pembimbing I

Pembimbing II



**Ahmad Fathurrozi, S.E., M.M.S.I.**  
NIDN. 0327117402



**Rakhmat Purnomo, S.Pd., S.Kom., M.Kom.**  
NIDN. 0322108201

## LEMBAR PENGESAHAN

Judul Skripsi : Penerapan Algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC dan *Secure Hash Algorithm* (SHA-256) Untuk Pengamanan Data File

Nama Mahasiswa : Selviyani

Nomor Pokok Mahasiswa : 201710225097

Program Studi / Fakultas : Informatika / Ilmu Komputer

Tanggal Lulus Ujian Skripsi : 14 Juli 2021

Bekasi, 19 Juli 2021

Mengesahkan,

Ketua Tim Penguji : **R. Wisnu Prio Pamungkas, S.Kom., M.Kom.** .....  
NIDN. 0321127201

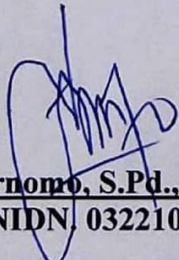
Penguji (I) : **Sugiyatno, S.Kom., M.Kom.** .....  
NIDN. 0313077206

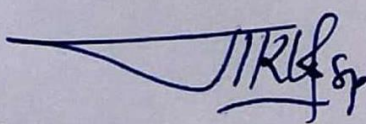
Penguji (II) : **Ahmad Fathurrozi, S.E., M.M.S.I.** .....  
NIDN. 0327117402

Mengetahui,

Ketua Program Studi  
Informatika

Dekan  
Fakultas Ilmu Komputer

  
**Rakhat Purnomo, S.Pd., S.Kom., M.Kom.**  
NIDN. 0322108201

  
**Herlawati, S.Si., M.M., M.Kom.**  
NIDN. 0311097302



## LEMBAR PERNYATAAN BUKAN PLAGIASI

Yang bertanda tangan dibawah ini :

Nama : Selviyani  
NPM : 201710225097  
Program Studi : Informatika  
Fakultas : Ilmu Komputer  
Judul Tugas Akhir : Penerapan Algoritma *Advanced Encryption Standard*  
(AES-256) Dengan Mode CBC dan *Secure Hash Algorithm*  
(SHA-256) Untuk Pengamanan Data File

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, 19 Juli 2021



Selviyani  
NPM 201710225097

## ABSTRACT

**Selviyani. 201710225097.** *The implementation of Advanced Encryption Standard (AES-256) Algorithm with CBC Mode and Secure Hash Algorithm (SHA-256) for Data File Security.*

*Data Security is one of the important things to protect important messages and information from corruption, compromise or loss so that messages and information remain safe. Encryption and decryption techniques are considered to be able to secure data properly by protecting files from being easily read or seen by unauthorized parties. In this case, the authors used data from University of Bhayangkara Jakarta Raya to be able to secure their university data using a cryptography symmetrical algorithm called Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) as a solution to existing problems. The AES algorithm process is divided into four steps, the first step is SubBytes, the second step is ShiftRows, the third step is MixColumns and the last step is AddRoundKey. And using the SHA algorithm as the hashing function. The algorithm is applied to a desktop-based file decryption and encryption application with the C sharp programming language.*

**Keywords:** *Data File Security, Encryption, Decryption, Algorithm AES-256, SHA-256*



## ABSTRAK

**Selviyani. 201710225097.** Penerapan Algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC dan *Secure Hash Algorithm* (SHA-256) Untuk Pengamanan Data File.

Pengamanan data atau *data protection* merupakan salah satu hal penting untuk melindungi pesan dan informasi penting dari korupsi, kompromi atau kerugian supaya pesan dan informasi tersebut tetap aman. Teknik enkripsi dan deskripsi dinilai dapat mengamankan data dengan tepat dengan melindungi file agar tidak mudah untuk dibaca atau dilihat oleh pihak yang tidak berwenang. Pada penelitian ini penulis menggunakan data dari Universitas Bhayangkara Jakarta Raya untuk dapat mengamankan data universitas mereka menggunakan algoritma kriptografi simetris *Advanced Encryption Standard* (AES) dan *Secure Hash Algorithm* (SHA) sebagai solusi untuk masalah yang ada. Proses algoritma AES sendiri terbagi menjadi empat langkah, langkah pertama yaitu *SubBytes*, langkah kedua *ShiftRows*, langkah ketiga *MixColumns* dan langkah terakhir yaitu *AddRoundKey*. Serta menggunakan algoritma SHA sebagai fungsi hashing-nya. Penerapan algoritma tersebut diterapkan ke dalam aplikasi enkripsi dan deskripsi file berbasis desktop dengan bahasa pemrograman C sharp.

Kata Kunci : Pengamanan Data, Enkripsi, Deskripsi, Algoritma AES-256, SHA-256

## LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

---

---

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

Nama : Selviyani  
NPM : 201710225097  
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 :

**”PENERAPAN ALGORITMA *ADVANCED ENCRYPTION STANDARD*  
(AES-256) DENGAN MODE CBC DAN *SECURE HASH ALGORITHM*  
(SHA-256) UNTUK PENGAMANAN DATA FILE”**

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.

Bekasi, 19 Juli 2021


Selviyani  
NPM 201710225097

## KATA PENGANTAR

Dengan mengucapkan puji syukur atas nikmat yang diberikan oleh Allah SWT, dan tak lupa sholawat serta salam semoga tercurah kepada Uswah Khasanah Rasulullah SAW. Penulis dapat menyelesaikan tugas akhir ini. Penulisan tugas akhir ini dilakukan dalam rangka memenuhi salah satu syarat akademik untuk mencapai gelar Sarjana Komputer Program Studi Informatika pada Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya. Penulis menyadari bahwa tanpa bantuan dan bimbingan dari beberapa pihak, tugas akhir skripsi ini tidak dapat diselesaikan dengan segera.

Oleh karena itu, penulis ingin menyampaikan ucapan terimakasih kepada semua pihak yang telah membantu dalam penyusunan Skripsi, dan penulis mengucapkan terimakasih kepada yang terhormat :

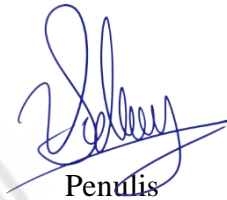
1. Bapak Irjen Pol. (Purn) Dr. Drs. Bambang Karsono, S.H., M.M selaku Rektor Universitas Bhayangkara Jakarta Raya.
2. Ibu Herlawati, S.Si., M.M., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
3. Bapak Rakhmat Purnomo, S.Pd., S.Kom., M.Kom., selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
4. Ibu Sri Rezeki, S.Kom., M.Kom., selaku Penasehat Akademik Kelas A2 angkatan 2017 Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
5. Bapak Ahmad Fathurrozi, S.E., M.M.S.I., selaku Dosen Pembimbing Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
6. Keluarga tercinta, Bapak dan Kakak yang selalu memberikan dukungan dan do'a untuk penulis.
7. Stephan Verbücheln yang selalu menemani dan memberi dukungan serta bantuan dalam menjalani proses penelitian ini.
8. Saudari Neina Corina, Eno Widyasari dan seluruh teman-teman seperjuangan di Program Informatika Angkatan 2017 yang selalu memberikan dukungan selama ini.



Karena kebaikan dari beliau-beliau, maka penulis dapat menyelesaikan skripsi ini dengan baik. Penulis menyadari bahwa penyusunan laporan ini tidak luput dari kesalahan dan kekurangan, maka dengan segala kerendahan hati, penulis menerima kritik dan saran yang membangun dari pembaca.

Akhir kata, semoga Allah Yang Maha Pengasih dan Maha Penyayang melimpahkan berkah dan anugerah-Nya kepada semua pihak dan membalas semua amal ibadahnya. Penulis berharap semoga Skripsi ini dapat memberikan manfaat bagi pihak yang memerlukan.

Bekasi, 19 Juli 2021



Penulis



# DAFTAR ISI

	Halaman
<b>LEMBAR PERSETUJUAN</b> .....	ii
<b>LEMBAR PENGESAHAN</b> .....	iii
<b>LEMBAR PERNYATAAN</b> .....	iv
<b>ABSTRAK</b> .....	v
<b>ABSTRACT</b> .....	vi
<b>LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI</b> .....	vii
<b>KATA PENGANTAR</b> .....	viii
<b>DAFTAR ISI</b> .....	x
<b>DAFTAR TABEL</b> .....	xiv
<b>DAFTAR GAMBAR</b> .....	xv
<b>DAFTAR LAMPIRAN</b> .....	xvi
<b>BAB I PENDAHULUAN</b> .....	1
1.1 Latar Belakang .....	1
1.2 Identifikasi Masalah .....	4
1.3 Rumusan Masalah .....	4
1.4 Tujuan dan Manfaat .....	4
1.5 Batasan Masalah .....	5
1.6 Tempat dan Waktu Penelitian .....	5
1.7 Sistematika Penulisan .....	6
<b>BAB II LANDASAN TEORI</b> .....	7
2.1 Kriptografi .....	7
2.2 Tujuan Kriptografi .....	7
2.3 Jenis Jenis Algoritma Kriptografi .....	8

2.4	Enkripsi dan Deskripsi .....	10
2.5	<i>Advanced Encryption Standard (AES-256)</i> .....	11
2.6	AES Mode CBC ( <i>Chiper Block Chaining</i> ) .....	12
2.7	<i>Padding</i> .....	13
2.8	<i>Key Schedule</i> .....	14
2.9	Proses Enkripsi .....	15
2.10	Proses Dekripsi .....	18
2.11	<i>Secure Hash Algorithm (SHA-256)</i> .....	20
2.12	Proses SHA-256 .....	22
2.13	<i>Unified Modelling Language (UML)</i> .....	23
2.14	<i>Use Case Diagram</i> .....	24
2.15	<i>Activity Diagram</i> .....	25
2.16	<i>Sequence Diagram</i> .....	26
2.17	Tinjauan Pustaka .....	27
<b>BAB III METODOLOGI PENELITIAN</b> .....		29
3.1	Objek Penelitian .....	29
3.2	Kerangka Penelitian .....	29
3.3	Metode Penelitian .....	34
3.4	Analisa Permasalahan .....	35
3.5	Analisa Sistem Yang Sedang Berjalan .....	35
3.6	Analisa Sistem Usulan .....	37
3.7	Analisa Kebutuhan Sistem .....	37
	3.7.1 Flowchart Aplikasi <i>Secret Fichier</i> .....	40
3.8	Alat Penelitian .....	41
3.9	Jadwal Penelitian .....	41

<b>BAB IV PERANCANGAN SISTEM DAN IMPLEMENTASI</b> .....	42
4.1 Penerapan <i>Secure Hash Algorithm</i> (SHA-256) .....	42
4.2 Penerapan <i>Advanced Encryption Standard</i> (AES-256) .....	46
4.2.1 Enkripsi File .....	46
4.2.2 Enkripsi Blok Pertama .....	49
4.2.3 Enkripsi Blok Kedua .....	75
4.2.4 Dekripsi File .....	88
4.2.5 Dekripsi Blok Pertama .....	90
4.2.6 Dekripsi Blok Kedua .....	108
4.3 Perancangan Aplikasi .....	112
4.3.1 <i>Use Case</i> .....	112
4.3.2 <i>Activity Diagram</i> .....	114
4.3.2.1 <i>Activity Diagram</i> Enkripsi File .....	114
4.3.2.2 <i>Activity Diagram</i> Dekripsi File .....	116
4.3.3 <i>Sequence Diagram</i> .....	117
4.3.3.1 <i>Sequence Diagram</i> Enkripsi File .....	117
4.3.3.2 <i>Sequence Diagram</i> Dekripsi File .....	118
4.4 Perancangan Antar Muka Aplikasi ( <i>User Interface</i> ) .....	119
4.4.1 Desain Tampilan Awal ( <i>Form Dashboard</i> ) .....	119
4.4.2 Desain Tampilan Menu Proses ( <i>Form Process</i> ) .....	120
4.4.3 Desain Tampilan Keterangan Aplikasi ( <i>Form About</i> ) .....	120
4.5 Fase Implementasi .....	121
4.6 Implementasi Perangkat Lunak .....	121
4.7 Implementasi Perangkat Keras .....	122
4.8 Implementasi Aplikasi .....	122

4.8.1	<i>Form Dashboard</i> .....	122
4.8.2	<i>Form Process</i> .....	122
4.8.3	<i>Form About</i> .....	123
4.9	Penerapan SHA-256 dan AES-256 Mode CBC Dalam Program .....	124
4.10	Hasil Pengujian .....	124
<b>BAB V PENUTUP</b> .....		129
5.1	Kesimpulan .....	129
5.2	Saran .....	130

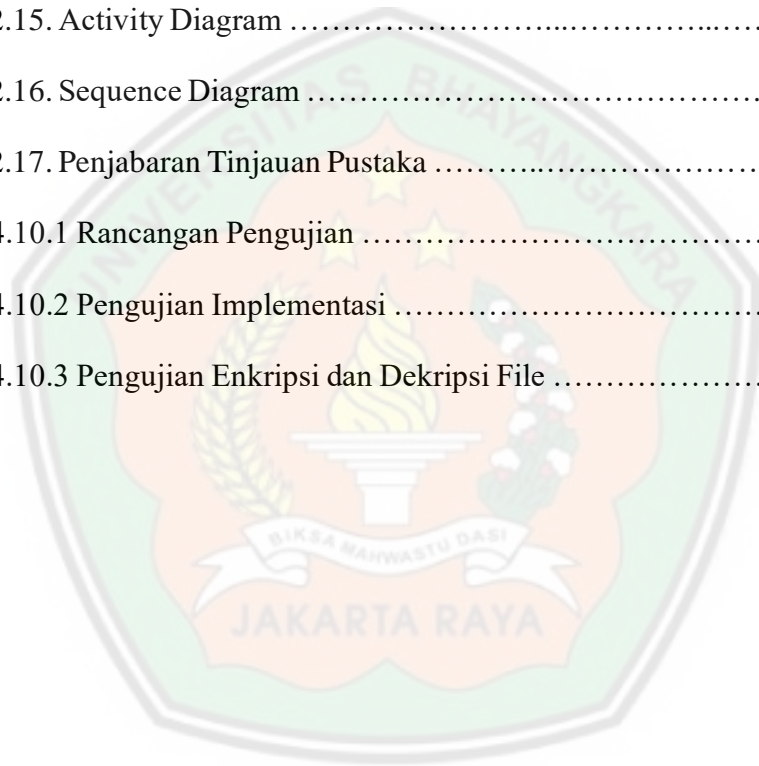
**DAFTAR PUSTAKA**

**LAMPIRAN**



## DAFTAR TABEL

	Halaman
Tabel 2.5. Perbandingan Jumlah Key & Round Algoritma AES .....	12
Tabel 2.8.1. Tabel Rcon .....	15
Tabel 2.9.1. Tabel S-box .....	16
Tabel 2.10.3. Tabel Inverse S-box .....	19
Table 2.14. Use Case Diagram .....	24
Tabel 2.15. Activity Diagram .....	25
Tabel 2.16. Sequence Diagram .....	26
Tabel 2.17. Penjabaran Tinjauan Pustaka .....	27
Tabel 4.10.1 Rancangan Pengujian .....	125
Tabel 4.10.2 Pengujian Implementasi .....	125
Tabel 4.10.3 Pengujian Enkripsi dan Dekripsi File .....	128



## DAFTAR GAMBAR

	Halaman
Gambar 2.3.1. Algoritma Simetris .....	8
Gambar 2.3.2. Algoritma Asimetris .....	9
Gambar 2.4. Proses Enkripsi dan Deskripsi .....	11
Gambar 2.5. Mode Operasi <i>Chiper Block Chaining</i> .....	13
Gambar 2.8. Proses <i>Key Schedule</i> .....	14
Gambar 2.9.2. Tahapan Proses ShiftRows .....	16
Gambar 2.9.3. Tahapan Proses MixColumns .....	16
Gambar 2.9. Alur Proses Enkripsi AES-256 .....	17
Gambar 2.10.2. Tahapan Proses Inverse ShiftRows .....	18
Gambar 2.10.4. Tahapan Proses Inverse MixColumns .....	19
Gambar 2.10 Alur Proses Dekripsi AES-256 .....	20
Gambar 2.11 Alur Proses Algoritma Hashing .....	22
Gambar 3.2. Kerangka Penelitian .....	29
Gambar 3.2. Kerangka Penelitian (Lanjutan) .....	30
Gambar 3.5.1 Use Case Sistem Berjalan .....	36
Gambar 3.5.2 Activity Diagram Sistem Berjalan .....	36
Gambar 3.5.3 Sequence Diagram Sistem Berjalan .....	36
Gambar 3.6.1 Use Case Sistem Usulan .....	37
Gambar 3.6.2 Activity Diagram Sistem Usulan .....	37
Gambar 3.7.1. Flowchart Enkripsi dan Dekripsi File .....	40
Gambar 4.2.3 Hasil Enkripsi .....	88
Gambar 4.2.6 Hasil Dekripsi .....	111
Gambar 4.3.1. <i>Use Case Diagram Secret Fichier</i> .....	113

Gambar 4.3.2.1. <i>Diagram Activity</i> Enkripsi File .....	114
Gambar 4.3.2.2. <i>Diagram Activity</i> Dekripsi File .....	116
Gambar 4.3.3.1. <i>Sequence Diagram</i> Enkripsi File .....	117
Gambar 4.3.3.2. <i>Sequence Diagram</i> Dekripsi File .....	118
Gambar 4.4.1. Desain Form <i>Dashboard</i> .....	119
Gambar 4.4.2. Desain Form <i>Process</i> .....	120
Gambar 4.4.3. Desain Form <i>About</i> .....	120
Gambar 4.8.1. Tampilan Form <i>Dashboard</i> .....	122
Gambar 4.8.2. Tampilan Form <i>Process</i> .....	123
Gambar 4.8.3 Tampilan Form <i>About</i> .....	123





## DAFTAR LAMPIRAN

1. Surat Permohonan Mengambil Data Penelitian
2. Plagiarism Cek
3. Biodata Diri
4. Kartu Bimbingan Skripsi

