



**IMPLEMENTASI ALGORITMA AES DAN BCRYPT UNTUK  
PENGAMANAN FILE DOKUMEN**

**SKRIPSI**

**GEBRINA DIVVA MEUTHIA ZULMA**

**1710511011**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA  
2022**



**IMPLEMENTASI ALGORITMA AES DAN BCRYPT UNTUK  
PENGAMANAN FILE DOKUMEN**

**SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana  
Komputer**

**GEBRINA DIVVA MEUTHIA ZULMA**

**1710511011**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA**

**2022**

## PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Gebrina Divva Meuthia Zulma

NIM : 1710511011

Tanggal : 1 Juli 2022

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 1 Juli 2022

Yang Menyatakan

  


(Gebrina Divva Meuthia Zulma)

## PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta,  
saya yang bertanda tangan dibawah ini:

Nama : Gebrina Divva Meuthia Zulma

NIM : 1710511011

Fakultas : Ilmu Komputer

Program Studi : Informatika

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

### **Implementasi Algoritma AES dan Bcrypt Untuk Pengamanan File Dokumen**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 1 Juli 2022

Yang Menyatakan



(Gebrina Divva Meuthia Zulma)

## LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa skripsi berikut:

Nama : Gebrina Divva Meuthia Zulma  
NIM : 1710511011  
Program Studi : Ilmu Komputer  
Konsentrasi : Informatika  
Judul Skripsi : Implementasi Algoritma AES dan Bcrypt Untuk Pengamanan File Dokumen

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Bayu Hananto, S.Kom., M.Kom.  
Penguji I



Yuni Widiastiwi, S.Kom., M.Si.  
Penguji II



Henki Bayu Seta, S.Kom., M.TI.  
Dosen Pembimbing I



Dr. Ermaita, M.Kom.  
Dekan



Desta Sandya Prasvita, M.Kom.  
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Ujian : 1 Juli 2022



# **Implementasi Algoritma AES dan Bcrypt Untuk Pengamanan File Dokumen**

**Gebrina Divva Meuthia Zulma**

## **ABSTRAK**

Dengan perkembangan kasus Covid-19 saat ini, masyarakat dihimbau untuk mengurangi aktivitas diluar, sehingga Microsoft Office dan pdf menjadi sangat penting untuk pertukaran data. Sayangnya data tersebut menjadi rentan terhadap serangan, sehingga dibutuhkan kriptografi agar file dokumen dapat terlindungi.

Perlu dibuat suatu aplikasi berbasis *web* menggunakan *framework* Laravel dimana *file* dokumen akan dienkripsi menggunakan AES 256 lalu *secret key* tersebut akan di *hashing* menggunakan Bcrypt .Hasil penelitian yang diharapkan yaitu sebuah *web* yang dapat digunakan untuk pengamanan *file* dokumen menggunakan AES dan Bcrypt.

Kata kunci: AES, Bcrypt, *file* dokumen, pengamanan

# **Implementation of AES and Bcrypt Algorithms for Document File Security**

**Gebrina Divva Meuthia Zulma**

## **ABSTRACT**

*With the current development of Covid-19 case, The public is advised to reduce outside activities, so Microsoft Office and PDF are very important for data exchange. Unfortunately, the data becomes vulnerable to attack, so cryptography is needed so that document files can be protected.*

*It is necessary to make a web-based application using the Laravel framework where document files will be encrypted using AES 256 then the secret key will be hashed using Bcrypt. The expected results of the research are a web that can be used to secure document files using AES and Bcrypt.*

**Keywords:** AES, Bcrypt, *document files, security*

## **KATA PENGANTAR**

Puji dan syukur penulis panjatkan kepada Allah SWT yang Maha Esa karena telah melimpahkan karunia dan rahmatnya sehingga penulis dapat mengerjakan dan menyelesaikan skripsi ini dalam keadaan sehat secara jasmani dan rohani. Skripsi ini dibuat dan disusun dalam rangka untuk menyelesaikan pendidikan penulis yang digunakan sebagai salah satu syarat Tugas Akhir untuk lulus dari Program Studi S1 Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta. Tidak lupa penulis memberikan ucapan terima kasih atas doa, dukungan serta bimbingan-bimbingan yang penulis sangat butuhkan, terutama untuk:

1. Seluruh orang tua dan nenek penulis yang tidak berhenti percaya, mendukung dan berdoa agar skripsi dapat diselesaikan dengan baik.
2. Ibu Dr. Ermatita, M.Kom., selaku dekan Fakultas Ilmu Komputer.
3. Bapak Desta Sandya Prasvita, M.Kom, selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
4. Bapak Henki Bayu Seta, S.Kom., M.TI. selaku Dosen Pembimbing yang telah memberikan waktu dan ilmunya untuk membimbing penulis dalam menyelesaikan skripsi tahun ini.
5. Bapak Toras Pangidoan Batubara, S.Si., M.Kom. yang melalui tesisnya telah membuka jalan awal bagi saya untuk menulis skripsi ini.
6. Dosen-dosen Program S1 Informatika Universitas Pembangunan Nasional Veteran Jakarta yang telah berjasa dalam membagikan ilmunya yang sangat bermanfaat bagi penulis dan mahasiswa/i lainnya.
7. Pihak lainnya yang tidak bisa disebutkan satu persatu tanpa mengurangi rasa hormat, penulis mengucapkan terima kasih yang sebesar-besarnya karena telah membantu penulis untuk menyelesaikan skripsi ini.



Melalui perjuangan dalam menyelesaikan skripsi ini, penulis menyadari bahwa skripsi merupakan langkah yang sangat penting dalam perkembangan ilmu teknologi dan informasi, sehingga penulis berharap karya tulis ini bisa bermanfaat dan berguna terutama bagi penelitian yang akan menggunakan skripsi ini sebagai salah satu sumbernya. Penulis menyadari bahwa skripsi yang telah disusun ini masih memiliki kekurangan, baik dari isi maupun cara penyampaiannya. Oleh karena itu, diharapkan terdapat saran serta kritik yang bisa digunakan untuk menyempurnakan dan menyelesaikan skripsi ini dengan baik. Akhir kata, semoga skripsi dengan judul “Implementasi Algoritma AES dan Bcrypt Untuk Pengamanan File Dokumen” bermanfaat dalam menambah ilmu dan wawasan bagi pembacanya dari segala kalangan, usia serta latar belakang pendidikannya lainnya.

Jakarta, 4 Juni 2022

A handwritten signature in black ink, appearing to read 'Divva', with a horizontal line underneath it.

Gebrina Divva Meuthia Zulma

## DAFTAR ISI

PERNYATAAN ORISINALITAS .....	i
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS .....	ii
LEMBAR PENGESAHAN .....	iii
ABSTRAK .....	iv
ABSTRACT .....	v
KATA PENGANTAR.....	vi
DAFTAR ISI .....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL .....	xii
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan dan Manfaat Penelitian .....	3
1.5 Sistematika Penulisan.....	4
BAB II LANDASAN TEORI .....	5
2.1 Kriptografi.....	5
2.1.1 Algoritma Simetris .....	6
2.1.2 Algoritma Asimetris .....	7
2.2 Hash.....	8
2.3 AES .....	9
2.4 Bcrypt.....	11
2.5 Penelitian Terdahulu .....	14
BAB III METODOLOGI PENELITIAN .....	19
3.1 Kerangka Pikir .....	19
3.2 Tahapan Penelitian .....	20
3.2.1 Identifikasi Masalah .....	20
3.2.2 Studi Literatur .....	20

3.2.3	Analisis Sistem.....	20
3.2.4	Perancangan Aplikasi.....	20
3.2.5	Implementasi.....	21
3.2.6	Pengujian Sistem.....	23
3.2.7	Hasil dan Pembahasan.....	24
3.3	Perangkat yang Digunakan.....	24
3.3.1	Perangkat Keras.....	24
3.3.2	Perangkat Lunak.....	25
3.4	Jadwal Penelitian.....	26
<b>BAB IV HASIL DAN PEMBAHASAN.....</b>		<b>27</b>
4.1	Analisis Sistem.....	27
4.2	Flow Chart, Activity Diagram dan Use Case.....	29
4.2.1	Flowchart Register.....	29
4.2.2	Flowchart Login.....	30
4.2.3	Flowchart Enkripsi File dan Hashing Key.....	30
4.2.4	Flowchart Dekripsi File dan Cek Secret Key.....	32
4.2.5	Activity Diagram Register.....	33
4.2.6	Activity Diagram Login.....	34
4.2.7	Activity Diagram Enkripsi File dan Hashing Key.....	35
4.2.8	Activity Diagram Dekripsi File dan Cek Secret Key.....	36
4.2.9	Use Case.....	37
4.3	Penggunaan Algoritma AES pada Enkripsi dan Dekripsi File.....	38
4.3.1	Enkripsi File Menggunakan AES.....	38
4.3.2	Dekripsi File Menggunakan AES.....	50
4.4	Penggunaan Algoritma Bcrypt pada Hashing Key.....	58
4.5	Tampilan Antarmuka.....	69
4.5.1	Register.....	69
4.5.2	Login.....	69
4.5.3	Dashboard.....	70
4.5.4	Menu Utama.....	71
4.6	Analisis Data.....	74

4.6.1	Pengujian Besar Data .....	74
4.6.2	Pengujian Waktu .....	75
4.6.3	Pengujian Integritas File dan Secret Key .....	85
BAB V Kesimpulan dan Saran.....		89
5.1	Kesimpulan .....	89
5.2	Saran.....	90
DAFTAR PUSTAKA.....		91
LAMPIRAN .....		96

## DAFTAR GAMBAR

Gambar 2.1 Skema Fungsi Algoritma Simetris.....	6
Gambar 2.2 Skema Fungsi Algoritma Asimetris .....	7
Gambar 2.3 Diagram Proses Enkripsi .....	10
Gambar 2.4 Struktur Bcrypt .....	12
Gambar 2.5 Langkah <i>Hashing</i> Bcrypt.....	13
Gambar 3.1 Kerangka Pikir .....	19
Gambar 3.2 Flowchart Sistem .....	22
<a href="#">Gambar 4.1 <i>Flowchart Register</i></a> .....	29
<a href="#">Gambar 4.2 <i>Flowchart Login</i></a> .....	30
<a href="#">Gambar 4.3 <i>Flowchart Enkripsi File dan Hashing Secret Key</i></a> .....	31
<a href="#">Gambar 4.4 <i>Flowchart Dekripsi File dan Cek Secret Key</i></a> .....	32
<a href="#">Gambar 4.5 <i>Activity Diagram Register</i></a> .....	33
<a href="#">Gambar 4.6 <i>Activity Diagram Login</i></a> .....	34
<a href="#">Gambar 4.7 <i>Activity Diagram Enkripsi File dan Hashing Secret Key</i></a> .....	35
<a href="#">Gambar 4.8 <i>Activity Diagram Dekripsi File dan Cek Secret Key</i></a> .....	36
<a href="#">Gambar 4.9 <i>Use Case Sistem</i></a> .....	37
<a href="#">Gambar 4.10 Register</a> .....	69
<a href="#">Gambar 4.11 Login</a> .....	70
<a href="#">Gambar 4.12 Dashboard</a> .....	70
<a href="#">Gambar 4.13 Sidebar</a> .....	71
<a href="#">Gambar 4.14 Menu PDF</a> .....	71
<a href="#">Gambar 4.15 Menu DOCX</a> .....	71
<a href="#">Gambar 4.16 Menu New File</a> .....	72
<a href="#">Gambar 4.17 Menu Enkrip</a> .....	72
<a href="#">Gambar 4.18 Menu Get Key</a> .....	72
<a href="#">Gambar 4.19 Status File</a> .....	73
<a href="#">Gambar 4.20 Dekripsi File</a> .....	73
<a href="#">Gambar 4.21 File Kembali Seperti Semula</a> .....	73
<a href="#">Gambar 4.22 Powershell Hasil Pengecekan <i>Hash</i> Pada <i>File</i></a> .....	85

## DAFTAR TABEL

Tabel 2.1 Panjang Kunci, Ukuran Blok dan Jumlah Putaran .....	9
Tabel 2.2 Penelitian Terdahulu.....	16
Tabel 3.1 Jadwal Penelitian .....	26
Tabel 4.1 Field dari tabel <i>files</i> .....	27
Tabel 4.2 Tabel Rcon .....	41
Tabel 4.3 Pengujian Besar File Tipe Pdf.....	74
Tabel 4.4 Pengujian Besar File Tipe Docx.....	75
Tabel 4.5 Pengujian Waktu Tipe Pdf Komputer 1 .....	76
Tabel 4.6 Pengujian Waktu Tipe Docx Komputer 1 .....	76
Tabel 4.7 Pengujian Waktu Tipe Pdf Komputer 2 .....	77
Tabel 4.8 Pengujian Waktu Tipe Docx Komputer 2 .....	77
Tabel 4.9 Rata-rata Lama Waktu Penggunaan AES Pada Pengamanan File .....	78
Tabel 4.10 Waktu Penggunaan Bcrypt Untuk Pengamanan <i>Secret Key</i> Komputer 1 Pada <i>File Pdf</i> .....	79
Tabel 4.11 Waktu Penggunaan Bcrypt Untuk Pengamanan <i>Secret Key</i> Komputer 1 Pada <i>File Docx</i> .....	79
Tabel 4.12 Waktu Penggunaan Bcrypt Untuk Pengamanan <i>Secret Key</i> Komputer 2 Pada <i>File Pdf</i> .....	80
Tabel 4.13 Waktu Penggunaan Bcrypt Untuk Pengamanan <i>Secret Key</i> Komputer 2 Pada <i>File Docx</i> .....	80
Tabel 4.14 Presentase Peningkatan Waktu Penggunaan Bcrypt Untuk Pengamanan <i>Secret Key</i> Komputer 1 Pada <i>File Pdf</i> .....	81
Tabel 4.15 Presentase Peningkatan Waktu Penggunaan Bcrypt Untuk Pengamanan <i>Secret Key</i> Komputer 1 Pada <i>File Docx</i> .....	82
Tabel 4.16 Presentase Peningkatan Waktu Penggunaan Bcrypt Untuk Pengamanan <i>Secret Key</i> Komputer 2 Pada <i>File Pdf</i> .....	82
Tabel 4.17 Presentase Peningkatan Waktu Penggunaan Bcrypt Untuk Pengamanan <i>Secret Key</i> Komputer 2 Pada <i>File Docx</i> .....	83
Tabel 4.18 Lama Waktu Yang Dibutuhkan untuk Setiap Kombinasi Kunci pada Komputer 1 Jenis <i>File Docx</i> .....	83

Tabel 4.19 Lama Waktu Yang Dibutuhkan untuk Setiap Kombinasi Kunci pada Komputer 1 Jenis <i>File Pdf</i> .....	84
Tabel 4.20 Lama Waktu Yang Dibutuhkan untuk Setiap Kombinasi Kunci pada Komputer 2 Jenis <i>File Docx</i> .....	84
Tabel 4.21 Lama Waktu Yang Dibutuhkan untuk Setiap Kombinasi Kunci pada Komputer 2 Jenis <i>File Pdf</i> .....	85
Tabel 4.22 Perbandingan Hasil Hash di Dalam File Berbentuk Heksadesimal .....	86
Tabel 4.23 Perbandingan Output Heksadesimal Sebelum dan Sesudah di Hash .....	87