

**LAPORAN AKHIR**

**APLIKASI SISTEM KEAMANAN DATA DENGAN METODE AES  
BERBASIS WEB**



**Laporan ini disusun untuk memenuhi syarat menyelesaikan  
Pendidikan Diploma III Jurusan Teknik Komputer  
Politeknik Negeri Sriwijaya**

**Oleh :**

**Dimas Andhika Pradana**

**061830700498**

**JURUSAN TEKNIK KOMPUTER  
POLITEKNIK NEGERI SRIWIJAYA**

**2021**

**LEMBAR PERSETUJUAN LAPORAN AKHIR**  
**APLIKASI SISTEM KEAMANAN DATA DENGAN METODE**  
**AES BERBASIS WEB**



Oleh :

**Dimas Andhika Pradana**

**061830700498**

Palembang, 18 Agustus 2021

**Pembimbing I**

**Pembimbing II**

**Ir. A. Bahri Joni Malvan, M. Kom.**

**M. Miftakul Amin, S.Kom., M.Eng.**

**NIP. 196007101991031001**

**NIP. 197912172012121001**

Mengetahui,

**Ketua Jurusan Teknik Komputer**

**Azwardi, ST., M.T**

**NIP. 197005232005011004**

APLIKASI SISTEM KEAMANAN DATA DENGAN METODE AES  
BERBASIS WEB



Telah diuji dan dipertahankan di depan dewan penguji pada sidang  
Laporan Akhir pada Hari Senin, 26 Juli 2021

Ketua Dewan Penguji

Ema Laila. S.Kom., M.Kom.

NIP. 197703292001122002

Anggota Dewan Penguji

Adi Sutrisman. S.Kom., M.Kom.

NIP. 197503052001121005

Ikhtison Mekongga. S.T., M.Kom

NIP. 197705242000031002

Isnainy Azro. S.Kom., M.Kom

NIP. 197310012002122007

Slamet Widodo. S.Kom., M.Kom

NIP. 197305162002121001

Tanda Tangan

Palembang, 18 Agustus 2021

Mengetahui,

Ketua Jurusan Teknik Komputer

Azwardi, ST., M.T

NIP. 197005232005011004



**KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN  
POLITEKNIK NEGERI SRIWIJAYA**

Jalan Srijaya Negara, Palembang 30139

Telp. 0711-353414 fax. 0711-355918

Website : [www.polsri.ac.id](http://www.polsri.ac.id) E-mail : [info@polsri.ac.id](mailto:info@polsri.ac.id)



**SURAT PERNYATAAN BEBAS PLAGIARISME**

Yang bertanda tangan di bawah ini :

Nama : Dimas Andhika Pradana  
NIM : 061830700498  
Jurusan / Program Studi : Teknik Komputer  
Judul Laporan Akhir : Aplikasi Sistem Keamanan Data Dengan Metode  
AES Berbasis Web.

Dengan ini menyatakan :

1. Laporan akhir yang saya buat dengan judul sebagaimana tersebut di atas beserta isinya merupakan hasil penelitian saya sendiri.
2. Laporan akhir tersebut bukan plagiat atau menyalin laporan akhir milik orang lain.
3. Apabila laporan akhir ini dikemudian hari dinyatakan plagiat atau menyalin laporan akhir milik orang lain, maka saya bersedia menanggung konsekuensinya.

Demikian surat pernyataan ini saya buat dengan sebenarnya untuk diketahui oleh pihak – pihak yang berkepentingan.

Palembang, 2021

Yang membuat pernyataan,

Dimas Andhika Pradana

NIM 061830700498

## MOTTO

“Karunia Allah yang paling lengkap adalah kehidupan yang didasarkan pada ilmu pengetahuan.”

*(Ali bin Abi Thalib)*

“Bermimpilah seakan kau akan hidup selamanya. Hiduplah seakan kau akan mati hari ini.”

**(Dimas Andhika Pradana)**

“Sukses adalah saat persiapan dan kesempatan bertemu.”

**(Dimas Andhika Pradana)**

Kupersembahkan untuk :

- ❖ Ayah dan Ibu Tersayang
- ❖ Keluargaku Tersayang
- ❖ Sahabat dan Teman Seperjuangan
- ❖ Almamaterku

**ABSTRAK**  
**APLIKASI SISTEM KEAMANAN DATA DENGAN METODE AES**  
**BERBASIS WEB**

---

**(Dimas Andhika Pradana, 2021:29)**

Laporan ini berjudul “Aplikasi Sistem Keamanan Data Dengan Metode AES Berbasis Web”. Aplikasi ini merupakan aplikasi yang dapat mengenkripsi dan mendekripsi file, dengan tujuan agar dapat mengamankan data dari penyalahgunaan, pengambilan, pengubahan data dari orang yang tidak bertanggung jawab. Pembuatan aplikasi ini menggunakan Macromedia Dreamweaver 8 dengan Bahasa pemrograman PHP, dan menggunakan database MySQL untuk penyimpanan data. Penelitian ini bertujuan untuk membuat sebuah sistem keamanan data dengan mengimplementasikan kriptografi pada file melalui perhitungan algoritma AES (Advanced Encryption Standard). Algoritma Advanced Encryption Standard (AES) adalah suatu algoritma block chipper dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi. Aplikasi ini menyediakan beberapa menu diantaranya menu login, menu enkripsi berkas, menu dekripsi berkas, dan menu daftar berkas. Hasil dari penelitian yaitu admin dapat melakukan enkripsi file dan file hasil enkripsi tersebut dapat di dekripsi kembali dengan file berformat sesuai extensi semula.

**Kata Kunci : Enkripsi, Dekripsi, Kriptografi, Advanced Encyption Standard.**

**ABSTRACT**  
**DATA SECURITY SYSTEM APPLICATION WITH AES METHOD**  
**WEB-BASED**

---

**(Dimas Andhika Pradana, 2021:29)**

This report is entitled “Application of Data Security System Using AES Web-Based Method”. This application is an application that can encrypt and decrypt files, with the aim of securing data from misuse, retrieval, alteration of data from irresponsible people. Making this application using Macromedia Dreamweaver 8 with PHP programming language, and using a MySQL database for data storage. This study aims to create a data security system by implementing cryptography on files through the calculation of the AES (Advanced Encryption Standard) algorithm. The Advanced Encryption Standard (AES) algorithm is a block cipher algorithm and has a symmetrical nature that uses a symmetric key during the encryption and decryption process. This application provides several menus including the login menu, file encryption menu, file decryption menu, and file list menu. The result of the research is that the admin can encrypt the file and the encrypted file can be decrypted again with the file format according to the original extension.

**Keywords: Encryption, Decryption, Cryptography, Advanced Encryption Standard.**

## KATA PENGANTAR

Alhamdulillah puji syukur penulis panjatkan kepada Allah SWT, karena berkat rahmat dan hidayah-Nya, penulis dapat menyelesaikan laporan akhir yang berjudul **“Aplikasi Sistem Keamanan Data Dengan Metode AES Berbasis Web”**.

Adapun maksud dan tujuan penulisan Laporan Akhir ini adalah sebagai syarat yang harus di penuhi untuk membuat Laporan Akhir yang merupakan salah satu mata kuliah yang harus dijalankan oleh mahasiswa untuk memenuhi kurikulum yang berlaku di Jurusan Teknik Komputer Politeknik Negeri Sriwijaya agar dapat menyelesaikan Program Studi Teknik Komputer untuk semester VI(enam).

Selama menyelesaikan Laporan Akhir ini penulis banyak sekali mendapat bantuan, bimbingan, semangat, petunjuk dari berbagai pihak, maka dalam kesempatan ini penulis ingin mengucapkan terimakasih kepada:

1. Allah SWT yang selalu mempermudah langkah untuk menyusun dan menyelesaikan Laporan Akhir.
2. Ayahku Ir. Zulkarnain, Ibuku Siti Mariam,S.H, Saudaraku M. Rafif Naufaldy yang selalu memberikan doa, dukungan, dan semangat yang tiada hentinya.
3. Bapak Dr. Ing. Ahmad Taqwa, M.T. selaku Direktur Politeknik Negeri Sriwijaya.
4. Bapak Azwardi, S.T., M.T selaku Ketua Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
5. Bapak Ir. A. Bahri Joni Malyan, M. Kom. selaku Dosen pembimbing I dan Bapak M. Miftakul Amin, S.Kom., M.Eng. yang telah memberikan arahan dan masukan dalam penyusunan Laporan Akhir ini.
6. Seluruh Dosen Teknik Komputer Politeknik Negeri Sriwijaya.
7. Teman-teman Jurusan Teknik Komputer Politeknik Negeri Sriwijaya terkhusus kelas CB angkatan 2018.
8. Seluruh orang-orang terdekat yang selalu memberikan dukungan dan semangat.

Penulis menyadari sepenuhnya bahwa masih banyak terdapat kekurangan dalam penyusunan laporan ini. Oleh karena itu, saran dan kritik yang bersifat membangun penulis harapkan.



Akhir kata mohon maaf atas segala kekurangan-kekurangan yang dilakukan praktikan dalam penyusunan laporan ini. Penulis berharap semoga Laporan Akhir ini dapat berguna dan bermanfaat khususnya bagi penulis dan umumnya bagi rekan-rekan mahasiswa Teknik Komputer Politeknik Negeri Sriwijaya sehingga tujuan yang diharapkan tercapai. Aamiin Ya Rabbal ‘Alamiin.

Palembang, 2021

Penulis

## DAFTAR ISI

<b>HALAMAN JUDUL</b> .....	i
<b>HALAMAN PERSETUJUAN</b> .....	ii
<b>HALAMAN PENGUJIAN</b> .....	iii
<b>SURAT PERNYATAAN BEBAS PLAGIARISME</b> .....	iv
<b>MOTTO</b> .....	v
<b>ABSTRAK</b> .....	vi
<b>ABSTRACT</b> .....	vii
<b>KATA PENGANTAR</b> .....	viii
<b>DAFTAR ISI</b> .....	x
<b>DAFTAR GAMBAR</b> .....	xii
<b>DAFTAR TABEL</b> .....	xiii

### **BAB I PENDAHULUAN**

1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan dan Manfaat .....	2
1.4.1 Tujuan .....	2
1.4.2 Manfaat .....	2

### **BAB II TINJAUAN PUSTAKA**

2.1 Landasan Teori.....	3
2.1.1 Kriptografi .....	3
2.1.2 Enkripsi dan Dekripsi .....	4
2.1.3 Algoritma AES .....	5
2.1.4 PHP .....	7
2.1.5 Macromedia Dreamweaver 8 .....	8
2.1.6 Database .....	9
2.1.7 MySQL .....	9
2.1.8 Black-box Testing .....	9
2.2 Referensi Jurnal .....	10

### **BAB III RANCANG BANGUN**

3.1 Metode Penelitian .....	12
3.2 Metode Pengujian .....	12
3.3 Kebutuhan Perangkat Lunak dan Perangkat Keras .....	13
3.4 Perancangan Sistem .....	13
3.5 Diagram Blok .....	13
3.6 Perancangan Flowchart .....	15
3.6.1 Flowchart Untuk Pengguna Aplikasi .....	15
3.7 Perancangan Database .....	16
3.8 Perancangan Aplikasi .....	17
3.8.1 Perancangan Form Login .....	17

3.8.2 Perancangan Form Enkripsi .....	18
3.9 Hasil Yang Diharapkan .....	19
<b>BAB IV HASIL DAN PEMBAHASAN</b>	
4.1 Hasil .....	20
4.1.1 Implementasi Basis Data .....	20
4.1.2 Tampilan Form Login .....	21
4.1.3 Tampilan Form Menu Utama Admin .....	22
4.1.4 Tampilan Form Menu Utama User .....	23
4.1.5 Tampilan Form Enkripsi Berkas .....	23
4.1.6 Tampilan Form Dekripsi Berkas .....	24
4.1.7 Tampilan Form Daftar Berkas .....	24
4.2 Hasil Pengujian .....	25
4.2.1 Tabel Hasil Pengujian .....	30
4.3 Pembahasan .....	30
<b>BAB V KESIMPULAN DAN SARAN</b>	
5.1 Kesimpulan .....	32
5.2 Saran .....	32
<b>DAFTAR PUSTAKA .....</b>	<b>33</b>
<b>LAMPIRAN</b>	

## DAFTAR GAMBAR

<b>Gambar 2.1</b>	Diagram Proses Enkripsi dan Dekripsi.....	5
<b>Gambar 2.2</b>	Proses Input Bytes, State Array, Output Bytes .....	6
<b>Gambar 2.3</b>	Proses Enkripsi Menggunakan Algoritma AES-128 .....	7
<b>Gambar 2.4</b>	Logo <i>PHP</i> .....	7
<b>Gambar 2.5</b>	Logo Aplikasi Macromedia Dreamweaver .....	8
<b>Gambar 3.1</b>	Diagram Blok Enkripsi dan Dekripsi .....	13
<b>Gambar 3.2</b>	Diagram Konteks Aplikasi Sistem Keamanan Metode AES ...	13
<b>Gambar 3.3</b>	Flowchart Pengguna Melakukan Enkripsi .....	14
<b>Gambar 3.4</b>	Flowchart Pengguna Melakukan Dekripsi .....	15
<b>Gambar 3.5</b>	Perancangan Form Login .....	17
<b>Gambar 3.6</b>	Perancangan Form Enkripsi .....	17
<b>Gambar 4.1</b>	Struktur Database keamanandata .....	18
<b>Gambar 4.2</b>	Struktur Tabel File .....	18
<b>Gambar 4.3</b>	Struktur Tabel User .....	19
<b>Gambar 4.4</b>	Tampilan Form Login .....	19
<b>Gambar 4.5</b>	Tampilan Form Login Jika Gagal Login .....	20
<b>Gambar 4.6</b>	Tampilan Form Utama Admin .....	20
<b>Gambar 4.7</b>	Tampilan Form Utama User .....	21
<b>Gambar 4.8</b>	Tampilan Form Enkripsi Berkas .....	21
<b>Gambar 4.9</b>	Tampilan Form Tabel Dekripsi Berkas .....	22
<b>Gambar 4.10</b>	Tampilan Form Dekripsi Berkas .....	22
<b>Gambar 4.11</b>	Tampilan Form Daftar Berkas .....	23
<b>Gambar 4.12</b>	Hasil Pengujian Login Berhasil Masuk (admin) .....	24
<b>Gambar 4.13</b>	Hasil Pengujian Login Berhasil Masuk (user) .....	24
<b>Gambar 4.14</b>	Hasil Pengujian Enkripsi Berkas .....	25
<b>Gambar 4.15</b>	Hasil Pengujian Berhasil Tersimpan .....	26
<b>Gambar 4.16</b>	Hasil Pengujian Dekripsi Berkas .....	27
<b>Gambar 4.17</b>	Hasil Pengujian Download Berkas .....	27

## DAFTAR TABEL

<b>Tabel 2.1</b>	Tabel Perbedaan Macam – Macam AES .....	5
<b>Tabel 2.2</b>	Daftar Referensi Jurnal .....	9
<b>Tabel 3.1</b>	Tabel Kebutuhan Perangkat Lunak .....	12
<b>Tabel 3.2</b>	Tabel File .....	16
<b>Tabel 3.3</b>	Tabel Users .....	16
<b>Tabel 4.1</b>	Fungsi Form Login .....	26
<b>Tabel 4.2</b>	Fungsi Form Enkripsi Berkas .....	27
<b>Tabel 4.3</b>	Fungsi Form Dekripsi Berkas .....	28
<b>Tabel 4.4</b>	Tabel Hasil Pengujian .....	30