

**PENERAPAN METODE AES UNTUK KEAMANAN
REPOSITORI DOKUMEN DIGITAL DI PENGADILAN
MILITER III-13 MADIUN**

SKRIPSI

Diajukan Sebagai Salah satu Syarat
Untuk Memperoleh Gelar Sarjana Jenjang Strata Satu (S1)
Pada Program Studi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Ponorogo



RENDY ARDICHA PRADANA
20533260

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH PONOROGO
2022**

HALAMAN PENGESAHAN

Nama : Rendy Ardicha Pradana
NIM : 20533260
Program Studi : Teknik Informatika
Fakultas : Teknik
Judul Proposal Skripsi : Penerapan Metode AES Untuk Keamanan
Repository Dokumen Digital di Pengadilan
Militer III-13 Madiun

Isi dan formatnya telah disetujui dan dinyatakan memenuhi syarat
Untuk melengkapi persyaratan guna memperoleh Gelar Sarjana
Pada Program Studi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Ponorogo

Ponorogo, 2022

Menyetujui,

Dosen Pembimbing I



Adi Fajaryanto Cobantoro, S.Kom., M.Kom
NIK. 1984092420130913

Dosen Pembimbing II



Moh. Bhanu Setyawan, ST., M.Kom
NIK. 1980022520130913

Mengetahui,

Dekan Fakultas Teknik,



Edy Kurniawan, S.T., M.T
NIK. 1977102620081012

Ketua Program Studi Teknik Informatika



Adi Fajaryanto Cobantoro, S.Kom., M.Kom
NIK. 1984092420130913

PERNYATAAN ORISINALITAS SKRIPSI

Yang bertanda-tangan dibawah ini :

Nama : Rendy Ardicha Pradana

NIM : 20533260

Prodi : Teknik-Informatika

Dengan ini menyatakan bahwa Skripsi saya dengan judul : “Penerapan Metode AES Untuk Keamanan Repositori Dokumen Digital di Pengadilan Militer III-13 Madiun” bahwa berdasarkan hasil penelusuran berbagai karya ilmiah, gagasan dan masalah ilmiah yang saya rancang / teliti didalam Naskah Skripsi ini adalah dari pemikiran saya. Tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata didalam Naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur plagiatisme, saya bersedia ijazah saya dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini dibuat dengan sesungguhnya dan dengan sebenar-benarnya.

Ponorogo, 2022



Rendy Ardicha Pradana

NIM. 20533260

HALAMAN BERITA ACARA UJIAN

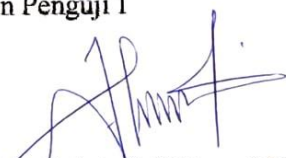
Nama : Rendy Ardicha Pradana
NIM : 20533260
Prodi : Teknik Informatika
Fakultas : Teknik
Judul Skripsi : Penerapan Metode AES Untuk Keamanan Repositori
Dokumen Digital di Pengadilan Militer III-13 Madiun

Telah diuji dan dipertahankan dihadapan
Dosen penguji tugas akhir jenjang Strata Satu (S1) pada :

Hari :
Tanggal :
Nilai :

Dosen Penguji

Dosen Penguji I


Indah Puji Astuti, S.Kom.,M.Kom.
NIK. 1986042420160913

Dosen Penguji II


Ismail Abdulrazzaq Z., S.Kom.,M.Kom
NIK.1988072820180313

Dekan Fakultas Teknik,


Edy Kurniawan, S.T.,M.T
NIK. 1977102620081012

Mengetahui,

Ketua Program Studi Teknik Informatika


Adi Fajaryanto Cobantoro, S.Kom., M.Kom
NIK. 1984092420130913

BERITA ACARA BIMBINGAN SKRIPSI

Nama : Rendy Ardicha Pradana

NIM : 20533260

Judul Skripsi : Penerapan Metode AES Untuk Keamanan Repositori Dokumen Digital di Pengadilan Militer III-13 Madiun

Dosen Pembimbing I : Adi Fajaryanto C., S.Kom., M.Kom.

PROSES BIMBINGAN

**BERITA ACARA
BIMBINGAN SKRIPSI**

Nama : Rendy Ardicha Pradana

NIM : 20533260

Judul Skripsi : _____

Dosen Pembimbing I : Adi Fajaryanto C., S.Kom., M.Kom.

PROSES PEMBIMBINGAN

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
1	16/12/22	Membaca	Membaca yang diarahkan ke dalam tugas yang diantar berkaitan	
2	17/12/22	Bab 1	ditambahkan referensi & lampiran Bab 3	
3	18/12/22	Bab 1 Bab 2 Bab 3	Bab 1 Acc Revisi minor Ditahan DFP & Fleaschart	
4	18/12/22	Bab 2 Bab 3 Bab 4	Bab 2 Acc Bab 3 Revisi Minor di minimal Waterfall	
5	19/12/22	Bab 3 Bab 4	Bab 3, 2, 4 Acc Ditahan Sampiran	
6	19/12/22	Format buku skripsi	Buku 1, 2, 3 kurang lebih sama seperti sampul Bab 4 berisi perkembangan dari apa yg dibuat	
7	21/12/22	Bab 4	Algoritma dapat disesuaikan dgn situasi & kondisi terkini	
8	22/12/22	Bab 4	Tampilkan pengujian terhadap algoritma AES	
9	27/12/22	Bab 4 Bab 5	- Aplikasi sudah ake - Lengkapi sesuai dgn format di buku panduan	
10	29/12/22	Bab 4 Bab 5 Lampiran	Bab 4 Acc Bab 5 Acc Bisa lanjut dapat saling Akhir	

BERITA ACARA BIMBINGAN SKRIPSI

Nama : Rendy Ardicha Pradana

NIM : 20533260

Judul Skripsi : Penerapan Metode AES Untuk Keamanan Repositori Dokumen Digital di Pengadilan Militer III-13 Madiun

Dosen Pembimbing II : Moh. Bhanu S., ST., M.Kom.

PROSES BIMBINGAN

BERITA ACARA BIMBINGAN SKRIPSI				
Nama		: Rendy Ardicha Pradana		
NIM		: 20533260		
Judul Skripsi		: Penerapan Metode AES Untuk Keamanan Repositori Dokumen Digital di Pengadilan Militer III-13 Madiun		
Dosen Pembimbing II		: Moh. Bhanu Setyawan, ST., M.Kom.		
PROSES PEMBIMBINGAN				
No	Tanggal	Materi Yang Dikonultasikan	Saran Pembimbing / Hasil	Tanda Tangan
1	12/07/2022	Bab 1	- konsistensi E-Court, file digital & tender yang di sital. - Rumusan masalah	
2	15/07/2022	Bab 2	- penelitian sejenis dan di cari perbedaannya	
3	18/07/2022	Bab 3	- revisi flow chart penelitian - rancangan pengujian algoritma	
4	07/07/22	Aplikasi	- sudah berjalan baik - hasil cari rekaman / log	
5	11/07/22		Bab 4 - hasil di perbaiki - masalah hasil dan bab	
6	12/07/22		Bab 5 - kesimpulan lebih detail - rumus masalah	
7	17/07/22		Acc aplikasi water mark	
8	14/07/22		Acc sidang	
9				
10				

ABSTRAK

PENERAPAN METODE AES UNTUK KEAMANAN REPOSITORI DOKUMEN DIGITAL DI PENGADILAN MILITER III-13 MADIUN

Rendy Ardicha Pradana, Adi Fajaryanto, M. Bhanu Setyawan

Program Studi Teknik Informatika, Fakultas Teknik, Universitas
Muhammadiyah Ponorogo

Email : rendy.altair@gmail.com

Abstrak.

Era revolusi industri 4.0 hadir dengan menitikberatkan pada otomasi dan digitalisasi antara pelaku industri dengan teknologi informasi. Semua instansi berlomba-lomba untuk *go-digital*. Tak terkecuali di dunia Peradilan, khususnya di Pengadilan Militer III-13 Madiun. Dulunya berkas perkara dicetak di kertas. Namun setelah kehadiran Sistem Informasi Penelusuran Perkara (SIPP), bisnis proses nya berubah. Selain harus dicetak di kertas, berkas perkara juga harus diupload kedalam aplikasi SIPP, sehingga mengharuskan untuk diubah kedalam file digital. Salah satu yang menjadi perhatian dalam penanganan file digital adalah tentang keamanan dan integritas datanya. Apakah dokumen ini benar dari pengirim aslinya? Apakah benar dokumen tersebut isinya belum dirubah oleh oknum yang tidak bertanggung jawab? Didalam skripsi ini, akan dilakukan penerapan *digital signature* berupa teknik enkripsi AES pada file putusan yang dihasilkan oleh Hakim. Tujuannya agar file tersebut aman dari serangan hacker dan tidak akan bisa dirubah isinya oleh oknum yang tidak bertanggung jawab, sehingga integritas datanya terjamin. Pengujian sistem dilakukan dengan membandingkan antara *plaintext* dan *ciphertext* yang dihasilkan oleh aplikasi. Dalam pengujian yang sudah dilakukan, terlihat ketika kita membuka *ciphertext* dengan aplikasi notepad, hasilnya adalah kumpulan huruf, simbol acak yang mustahil untuk dipahami oleh manusia. Ini membuktikan bahwasanya penggunaan aplikasi ini dapat mengamankan dokumen dengan baik dan mustahil untuk dibaca dan diganti isinya oleh *hacker*.

Kata kunci : AES, Ciphertext, Digital Signature, Dekripsi, Enkripsi

KATA PENGANTAR

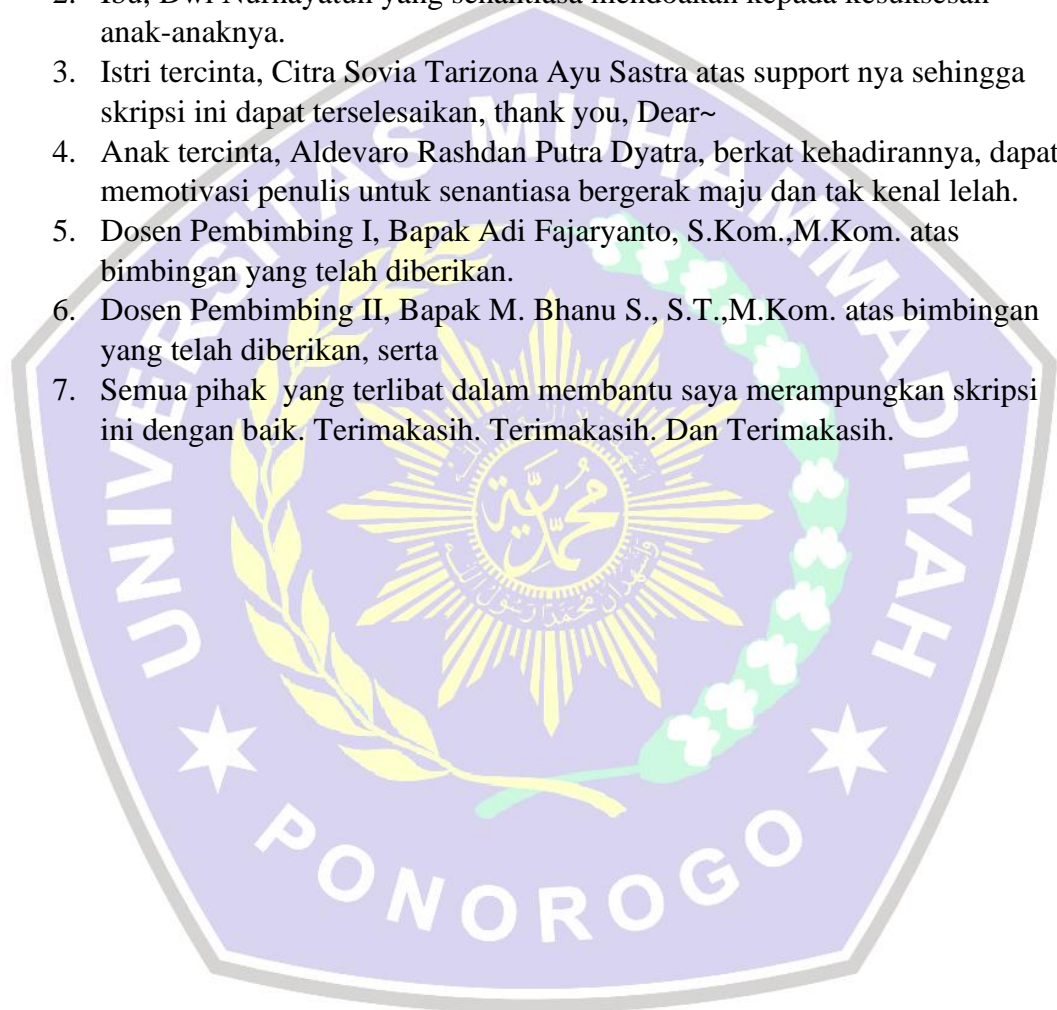
Didalam instansi pemerintahan, khususnya di dunia Peradilan, Putusan Pengadilan menentukan kualitas dari satuan kerja tersebut. Beragam inovasi dihadirkan untuk menjawab tantangan globalisasi dan digitisasi di era revolusi industri 4.0. Tak terkecuali penulis yang merupakan salah satu penggiat IT di instansi Pengadilan Militer III-13 Madiun. Penulis ingin menciptakan sebuah sistem, dimana arsip digital dapat disimpan dengan aman didalam ekosistem yang terkontrol sehingga tidak ada celah keamanan yang dapat dimasuki oleh *hacker* ataupun oknum yang tidak berwenang. Arsip digital dapat dijaga integritasnya, sehingga kualitas dari Instansi pun dapat terjaga, sehingga pencari keadilan dapat terpuaskan oleh kinerja Pengadilan yang adil dan prima.



UCAPAN TERIMA-KASIH.

Ucapan terima-kasih ini saya haturkan, kepada pihak-pihak yang telah sedikit-banyak membantu saya didalam proses untuk menyelesaikan skripsi ini, diantaranya :

1. Allah SWT, berkat ridho dan petunjuk-Nya lah, penelitian ini dapat dilancarkan dan paripurna.
2. Ibu, Dwi Nurhayatun yang senantiasa mendoakan kepada kesuksesan anak-anaknya.
3. Istri tercinta, Citra Sovia Tarizona Ayu Sastra atas support nya sehingga skripsi ini dapat terselesaikan, thank you, Dear~
4. Anak tercinta, Aldevaro Rashdan Putra Dyatra, berkat kehadirannya, dapat memotivasi penulis untuk senantiasa bergerak maju dan tak kenal lelah.
5. Dosen Pembimbing I, Bapak Adi Fajaryanto, S.Kom.,M.Kom. atas bimbingan yang telah diberikan.
6. Dosen Pembimbing II, Bapak M. Bhanu S., S.T.,M.Kom. atas bimbingan yang telah diberikan, serta
7. Semua pihak yang terlibat dalam membantu saya merampungkan skripsi ini dengan baik. Terimakasih. Terimakasih. Dan Terimakasih.



DAFTAR ISI

Contents

BERITA ACARA BIMBINGAN SKRIPSI	v
ABSTRAK	vii
KATA PENGANTAR	viii
UCAPAN TERIMA-KASIH.	ix
DAFTAR ISI.....	x
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN.....	xv
ARTI LAMBANG & SINGKATAN.....	xvi
BAB 1	1
PENDAHULUAN.....	1
1.1 LATAR-BELAKANG.....	1
1.2 PERUMUSAN MASALAH.....	2
1.3 TUJUAN PENELITIAN.....	2
1.4 BATASAN-MASALAH.....	2
1.5 MANFAAT-PENELITIAN.....	3
BAB 2	4
TINJAUAN PUSTAKA.....	4
2.1 Penelitian yang telah Dilakukan Sebelumnya	4
2.2 Landasan Teori	5
BAB 3	8
METODE PENELITIAN	8
3.1 Mulai.....	8
3.2 Pengumpulan Data.....	9
3.3 Analisa System Requirement.....	9
3.4 Perancangan Perangkat Lunak.....	11
3.5 Pengujian dan Pembuktian Algoritma	14
3.6 Pelaporan	14
BAB 4	16

ANALISA DATA DAN PEMBAHASAN	16
4.1 Tampilan Antarmuka	16
4.2 Pengujian Program.....	20
4.3 Pembuktian Algoritma AES	24
BAB 5	31
PENUTUP	31
5.1 Kesimpulan	31
5.2 Saran	31
DAFTAR PUSTAKA	32
DAFTAR LAMPIRAN.....	33



DAFTAR TABEL

Tabel 2.1 Penelitian Sebelumnya.....	4
Tabel 3.1 Rancangan Pengujian.....	16



DAFTAR GAMBAR

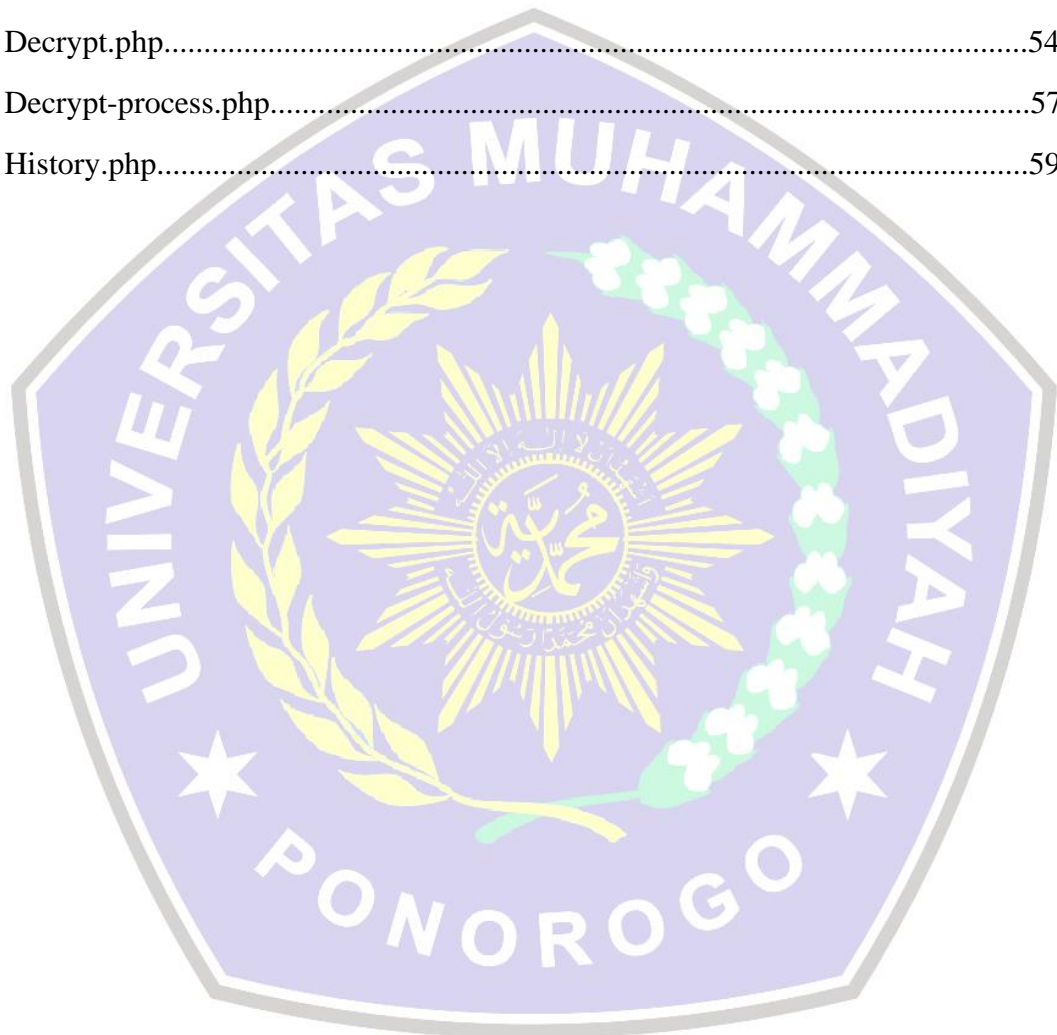
Gambar-3.1 Tahapan Penelitian.....	10
Gambar-3.2 Struktur Organisasi Pengadilan Militer III-13 Madiun.....	12
Gambar-3.3 Model Waterfall.....	13
Gambar-3.4 Diagram Konteks.....	14
Gambar-3.5 DFD Level 1.....	14
Gambar-3.6 Proses Penandatanganan dan Verifikasi.....	15
Gambar-4.1 Halaman Login Aplikasi.....	18
Gambar-4.2 Halaman Utama.....	18
Gambar-4.3 Halaman Enkripsi Berkas.....	19
Gambar-4.4 Contoh Error Bila Ekstensi Tidak Disupport.....	19
Gambar-4.5 Contoh Error Bila File Melebihi Kapasitas.....	20
Gambar 4.6 Proses Enkripsi Berhasil.....	20
Gambar 4.7 Sub Menu Dekripsi Berkas.....	20
Gambar 4.8 Proses Dekripsi Berkas.....	21
Gambar 4.9 Error Ketika Salah Input Password.....	21
Gambar 4.10 Menu Daftar Berkas Enkripsi dan Dekripsi.....	22
Gambar 4.11 Berkas Asli & Berkas Enkripsi.....	22
Gambar-4.12 Tampilan Asli dari File.....	23
Gambar-4.13 Status Terenkripsi pada Berkas yang Diunggah.....	23
Gambar-4.14 File Ciphertext.....	24
Gambar-4.15 Proses Dekripsi Berkas.....	24
Gambar 4.16 Password Tidak Sesuai.....	25
Gambar 4.17 Tombol Download Berkas.....	25
Gambar-4.18 File Hasil Dekripsi.....	25
Gambar-4.19 Tabel ASCII.....	27
Gambar-4.20 SBOX AES.....	28

Gambar 4.21 Proses Enkripsi.....	29
Gambar 4.22 Proses <i>Shift Row</i>	28
Gambar 4.23 Proses <i>Mix Columns</i>	28
Gambar 4.24 Proses <i>AddRoundKey</i>	29
Gambar 4.25 Hasil Round 2 menjadi Masukan di Round 3.....	29
Gambar 4.26 Round 10 (<i>Final Round</i>).....	30
Gambar 4.27 Hasil Akhir Proses Enkripsi.....	30



DAFTAR LAMPIRAN

Index.php.....	35
AES.php.....	37
Encrypt.php.....	49
Encrypt-process.php.....	52
Decrypt.php.....	54
Decrypt-process.php.....	57
History.php.....	59



ARTI LAMBANG & SINGKATAN

AES	: Advanced Encryption Standard
e-Court	: Electronic Court
IT	: Information Technology
DES	: <i>Data Encryption Standart</i>
MD5	: Message Digest 5
PHP	: PHP Hypertext Processor
DFD	: Data Flow Diagram
EXOR	: Exclussve OR

