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 Repositori 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	Dosen Pembimbing II
Adi Fajaryanto Cobantoro, S.Kom., M.Kom	Moh. Bhanu Setyawan, ST., M.Kom
NIK. 1984092420130913	NIK. 1980022520130913

Mengetahui,

Dekan Fakultas Teknik,	Ketua Program Studi Teknik Informatika
Edy Kurniawan, S.T.,M.T	Adi Fajaryanto Cobantoro, S.Kom., M.Kom
NIK. 1977102620081012	NIK. 1984092420130913

ii

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

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

iv

BERITA ACARA

BIMBINGAN SKRIPSI

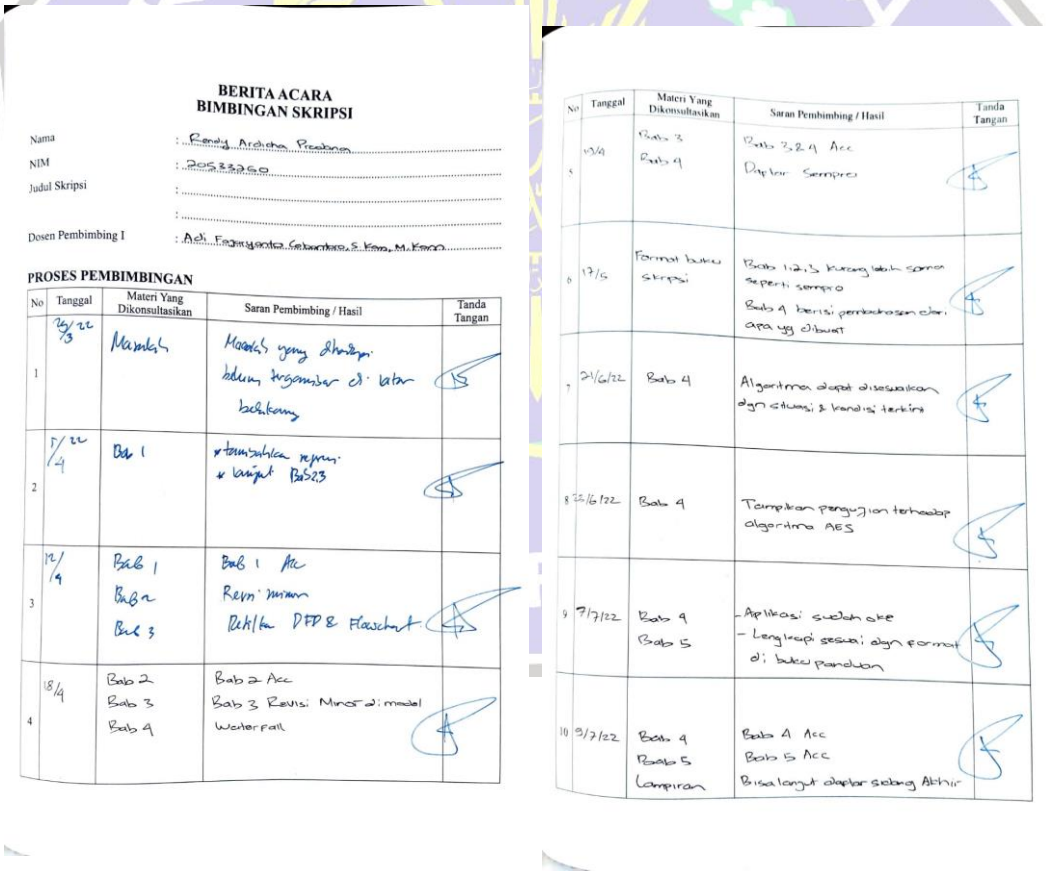
Nama : Rendy Ardicha Pradana

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 Cahyanto, S.Kom, M.Kom

PROSES PEMBIMBINGAN

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
1	26/3 22	Masalah	Masalah yang diangkat. Latar belakang tugasnya di latar belakang	
2	7/4 22	Bab 1	* tambahkan rujuk. * lanjut Bab 2,3	
3	12/4	Bab 1 Bab 2 Bab 3	Bab 1 Acc Revisi mirror Refleksi DFD & Flowchart	
4	18/4	Bab 2 Bab 3 Bab 4	Bab 2 Acc Bab 3 Revisi: Mirror di: modal Waterfall	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
5	03/4	Bab 3 Bab 4	Bab 3,2,4 Acc Daftar Sementara	
6	17/5	Format buku skripsi	Bab 1,2,3 kurang lebih sama seperti sempro Bab 4 berisi pembahasan dari apa yg dibuat	
7	21/6/22	Bab 4	Algoritma dapat disesuaikan dgn situasi & kondisi terkini	
8	23/6/22	Bab 4	Tampilan pengujian terhadap algoritma AES	
9	7/7/22	Bab 4 Bab 5	- Aplikasi sudah oke - Lengkapi sesuai dgn format di buku panduan	
10	9/7/22	Bab 4 Bab 5 Lampiran	Bab 4 Acc Bab 5 Acc Bisa lanjut daftar sidang Akhir	

BERITA ACARA

BIMBINGAN SKRIPSI

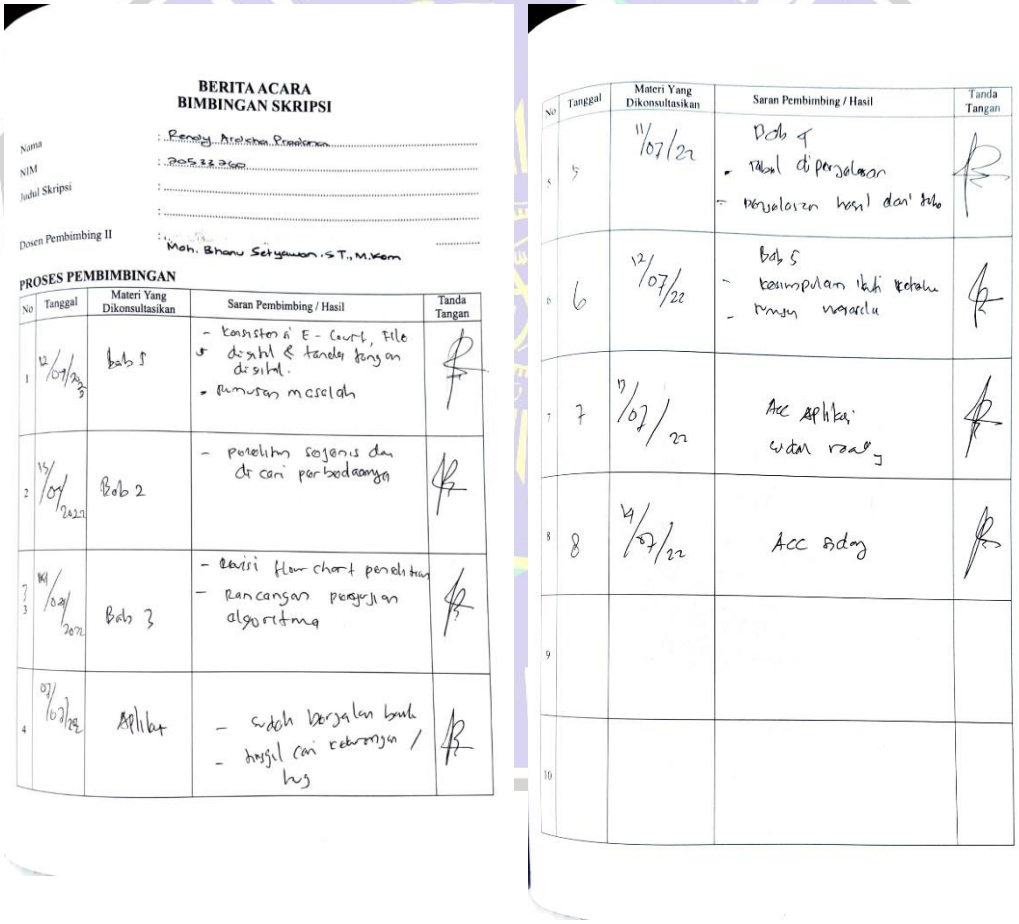
Nama : Rendy Ardicha Pradana

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 :
Dosen Pembimbing II : Moh. Bhanu Setyawan, S.T., M.Kom

PROSES PEMBIMBINGAN

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
1	12/07/2022	bab 1	- konsistensi E-Court, File digital & tanda tangan digital. - Rumusan masalah	
2	15/07/2022	Bab 2	- penelitian sejenis dan di cari perbedaannya	
3	18/07/2022	Bab 3	- tambah flow chart penelitian - Rancangan pengujian algoritma	
4	07/07/22	Aplikasi	- sudah berjalan baik - tinggal cari referensi / lain	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
5	5	11/07/22	Bab 4 - tabel di perjelas - penjelasan hasil dari tabel	
6	6	12/07/22	Bab 5 - kesimpulan lebih ringkas - saran ditambah	
7	7	17/07/22	Acc aplikasi sudah rapi	
8	8	19/07/22	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 digitlisasi 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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ARTI LAMBANG & SINGKATAN

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