

**IMPLEMENTASI *DIGITAL SIGNATURE* UNTUK TANDA
TANGAN SERTIFIKAT PESMA AL-MANAR
MENGGUNAKAN ALGORITMA RSA**

SKRIPSI

Diajukan Sebagai Salah Satu Syarat

Untuk Memperoleh Gelar Sarjana Jenjang Strata Satu (S1)

Pada Program Studi Teknik Informatika Fakultas Teknik

Universitas Muhammadiyah Ponorogo



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

HALAMAN PENGESAHAN

HALAMAN PENGESAHAN

Nama : Muhammad Dava Dharmawan
NIM : 18532988
Program Studi : Teknik Informatika
Fakultas : Teknik
Judul Skripsi : Implementasi *Digital Signature* Untuk Tanda
Tangan Sertifikat PESMA AL-MANAR
Menggunakan Algoritma RSA

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, 27 Juli 2022

Menyetujui,

Dosen Pembimbing I,



Adi Fajaryanto C., S.Kom., M.Kom
NIK. 19840924 201309 13

Dosen Pembimbing II,



Moh. Bhanu Setyawan, S.T., M.Kom
NIK. 19800225 201309 13

Mengetahui,

Dekan Fakultas Teknik,

Edy Kurniawan, S.T., M.T
NIK. 19771026 200810 12

Ketua Program Studi Teknik Informatika,


Adi Fajaryanto C., S. Kom., M.Kom
NIK. 19840924 201309 13

PERNYATAAN ORISINALITAS SKRIPSI

PERNYATAAN ORISINALITAS SKRIPSI

Yang bertanda tangan di bawah ini :

Nama : Muhammad Dava Dharmawan
NIM : 18532988
Program Studi : Teknik Informatika

Dengan ini menyatakan bahwa Skripsi saya dengan judul: " Implementasi *Digital Signature* Untuk Tanda Tangan Sertifikat PESMA AL-MANAR Menggunakan Algoritma RSA " bahwa berdasarkan hasil penelusuran berbagai karya ilmiah, gagasan dan masalah ilmiah yang saya rancang/teliti di dalam Naskah Skripsi ini adalah asli 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 di dalam Naskah Skripsi ini 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, 27 Juli 2022

Mahasiswa,



Muhammad Dava Dharmawan
NIM. 18532988

HALAMAN BERITA ACARA UJIAN

HALAMAN BERITA ACARA UJIAN

Nama : Muhammad Dava Dharmawan
NIM : 18532988
Program Studi : Teknik Informatika
Fakultas : Teknik
Judul Skripsi : Implementasi *Digital Signature* Untuk Tanda Tangan Sertifikat PESMA AL-MANAR Menggunakan Algoritma RSA

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

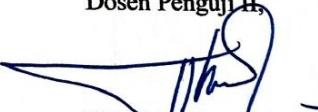
Hari : Selasa
Tanggal : 26 Juli 2022

Dosen Penguji,

Dosen Penguji I,


Indah Putri Astuti, S.Kom., M.Kom
NIK. 19860424 201609 13

Dosen Penguji II,


Ismail Abdulrazzaq Z., S.Kom, M.Kom
NIK. 19880728 201804 13

Mengetahui,


Dekan Fakultas Teknik,

Edy Kurniawan, S.T.,M.T
NIK. 19771026 200810 12

Ketua Program Studi Teknik Informatika,


Adi Fajaryanto C., S. Kom., M.Kom
NIK. 19840924 201309 13

BERITA ACARA BIMBINGAN SKRIPSI

BERITA ACARA BIMBINGAN SKRIPSI

Nama

NIM

Judul Skripsi

Dosen Pembimbing I

: MUHAMMAD DAVA DHARMAWAN

: 18532088

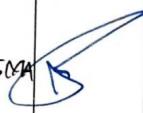
IMPLEMENTASI DIGITAL SIGNATURE UNTUK TANDA TANGAN SERTIFIKAT

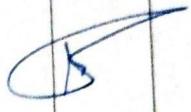
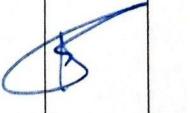
PESMA AL-MANAR MENGGUNAKAN ALGORITMA RSA

:

: Adi Fajaryanto C., S. Kom., M. Kom.

PROSES PEMBIMBINGAN

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
1	02/2022 /03	Konsultasi Bab I	Orientasi pada batar bataang dikuatkan, dengan penjabaran Apa itu PESMA, pentingnya PESMA dan mencantumkan masalah.	
2	21/2022 /03	Review Bab I	Sumber jurnal & Rumusan masalah	
3	29/2022 /03	Bab I	- Ace Bab I - Lanjut ke Bab II	
4	04/2022 /04	Bab II	- Ace Bab II - Pembahasan tinjauan pustaka.	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
5	05/2022 109'	Bab 3	Mulai membuat proto-type 1 hari membuat versi awal dgn bahan re	
6	12/22 14	Bab 3	tambahkan Referensi, Flowchart & Raster tabel	
7	19/22 14	Proposal	Ace Sembiring Rizqial	
8	03/22 05	Revisi Project	Terkait disederhanakan untuk gambar & teks harusnya dgn Verifikasi	
9	19/22 05	Penerapan Bab IV	lanjut naskah bab <u>IV</u> sertai Penambahan Saran.	
10	27/22 6	Naskah	- edit artikel - cek plagar.	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
11	6/22 7/7	Naskah	Naskah OK Pihgin Naskah OK kunj angka	
12	7/22 7/7		Acc today	
13				
14				
15				
16				

BERITA ACARA BIMBINGAN SKRIPSI

Nama

NIM

Judul Skripsi

Dosen Pembimbing II

: MUHAMMAD DAYA CHARMAWAN.

: 185329.R8

: IMPLEMENTASI DIGITAL SIGNATURE UNTUK TANDA TANGAN SERTIFIKAT
PESMA AL-MANAR MENGGUNAKAN ALGORITMA RSA

: Moh. Dhanu Setyawan, ST., M. Kom.

PROSES PEMBIMBINGAN

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
1	02/2022 /63	Konsultasi Judul	Cari banyak Referensi. D	
2	30/2022 /03	Revisi Bab I	Landasan Sertifikat elektronik Cari Referensinya. D SA	
3	05/2022 /09	Acc Bab I Revisi Bab II Revisi Bab III	Bab II Kasih Perbedaan didalam Tabel Penelitian. Bab III Kasih evaluasinya. D SA	
4	21/2022 /09	Proposal	Acc Seminar Proposal. D	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
5	19/06/22	Uji Coba Aplikasi	Penger 85% perbaiki dan siap notifikasi	R
6	11/06/22	Bab 1	- Data hasil uji coba di perbaiki	R
7	02/07/22	Aplikasi	Aplikasi sudah ok	R
8	03/07/22	Bab 5	Kesimpulan diambil berdasarkan hasil bab 4 & sistem dg labor bokabay	R
9	07/07/22	All	Ace sidang	R
10				

SURAT KETERANGAN HASIL PLAGIASI SKRIPSI



**UNIVERSITAS MUHAMMADIYAH PONOROGO
LEMBAGA LAYANAN PERPUSTAKAAN**
Jalan Budi Utomo 10 Ponorogo 63471 Jawa Timur Indonesia
Telp (0352) 481124, 487662 Fax (0352) 461796,
Website: library.umpo.ac.id
TERAKREDITASI A
(SK Nomor 00137/LAP.PT/III.2020)

**SURAT KETERANGAN
HASIL SIMILARITY CHECK KARYA ILMIAH MAHASISWA
UNIVERSITAS MUHAMMADIYAH PONOROGO**

Dengan ini kami nyatakan bahwa karya ilmiah dengan rincian sebagai berikut:

Nama : Muhammad Dava Dharmawan

NIM : 18532988

Prodi : Teknik Informatika

Judul : Implementasi Digital Signature Untuk Tanda Tangan Sertifikat PESMA AL-MANAR
Menggunakan Algoritma RSA

Dosen pembimbing :

1. Adi Fajaryanto C., S.Kom., M.Kom
2. Moh. Bhanu Setyawan, S.T., M.Kom

Telah dilakukan check plagiasi berupa SKRIPSI di L2P Universitas Muhammadiyah Ponorogo dengan prosentase kesamaan sebesar 20 %

Demikian keterangan ini dibuat untuk digunakan sebagaimana mestinya.

Ponorogo, 5 Juli 2022
Petugas pemeriksa



(Mohamad Ulil Albab,SIP)
NIK.1989092720150322

Nb: Dosen pembimbing dimohon untuk mengecek kembali keaslian soft file karya ilmiah yang telah diperiksa melalui Turnitin perpustakaan

SURAT KETERANGAN HASIL PLAGIASI ARTIKEL



UNIVERSITAS MUHAMMADIYAH PONOROGO
LEMBAGA LAYANAN PERPUSTAKAAN
Jalan Budi Utomo 10 Ponorogo 63471 Jawa Timur Indonesia
Telp (0352) 481124, 487662 Fax (0352) 461796,
Website: library.umpo.ac.id
TERAKREDITASI A
(SK Nomor 00137/LAP.PT/III.2020)

SURAT KETERANGAN HASIL SIMILARITY CHECK KARYA ILMIAH MAHASISWA UNIVERSITAS MUHAMMADIYAH PONOROGO

Dengan ini kami nyatakan bahwa karya ilmiah dengan rincian sebagai berikut:

Nama : Muhammad Dava Dharmawan

NIM : 18532988

Prodi : Teknik Informatika

Judul : IMPLEMENTASI DIGITAL SIGNATURE UNTUK TANDA TANGAN SERTIFIKAT PESMA AL-MANAR MENGGUNAKAN ALGORITMA RSA

Dosen pembimbing :

1. Adi Fajaryanto C., S.Kom., M.Kom

2. Moh. Bhanu Setyawan, S.T., M.Kom

Telah dilakukan check plagiasi berupa Artikel di L2P Universitas Muhammadiyah Ponorogo dengan prosentase kesamaan sebesar 21 %

Demikian keterangan ini dibuat untuk digunakan sebagaimana mestinya.

Ponorogo, 01 Agustus 2022
Petugas pemeriksa



(Mohamad Ulil Albab,SIP)
NIK.1989092720150322

Nb: Dosen pembimbing dimohon untuk mengecek kembali keaslian soft file karya ilmiah yang telah diperiksa melalui Turnitin perpustakaan

HALAMAN MOTTO

Sedikit Bila dihitung, Banyak Bila Dikumpulkan.

(Dzikrullah)



HALAMAN PERSEMBAHAN

Alhamdulillah tak lupa mengucapkan syukur kehadirat Allat SWT yang telah melimpahkan rahmat, taufiq serta hidayahnya sehingga dapat menyelesaikan pendidikan jenjang Strata Satu (S1) ini dengan segala kemudahan dan kelancaran menghadapi permasalahan yang ditemui. Untuk itu, saya persembahkan skripsi ini untuk :

1. Edy Kurniawan S.T., M.T selaku Dekan Teknik Informatika Universitas Muhammadiyah Ponorogo.
2. Adi Fajaryanto C, S. Kom, M.Kom selaku Kepala Prodi Teknik Informatika Universitas Muhammadiyah Ponorogo sekaligus dosen pembimbing I.
3. Moh. Bhanu Styawan, S.T, M.Kom selaku Dosen Pembimbing II yang telah sabar dan penuh perhatian memberikan bimbingan dan masukan yang bersifat membangun serta saran yang sangat bermanfaat bagi penulis dalam penyusunan Skripsi ini.
4. Ayah dan Ibu yang selalu memberikan do'a restu dan bantuan material serta nasihat-nasihat untuk selalu semangat dalam menuntut ilmu.
5. Sahabat dan teman seperjuangan di Teknik Informatika Universitas Muhammadiyah Ponorogo. Terutama untuk Kelas VIII D TI.
6. Teman-teman saya Andreas Mustofa, Satria Putra Perdana, Firmansyah Al-anshori.

Penulis menyadari bahwa dalam Skripsi ini masih jauh dari

kesempurnaan oleh karena itu kritik serta saran yang membangun sangat diharapkan demi kesempurnaan Skripsi ini.

Penulis berharap Skripsi ini dapat memberikan kontribusi positif pada perkembangan keilmuan dibidang Teknik Informatika dan Kesehatan serta bermanfaat bagi penulis dan semua pembacanya.



IMPLEMENTASI DIGITAL SIGNATURE UNTUK TANDA TANGAN
SERTIFIKAT PESMA AL-MANAR MENGGUNAKAN
ALGORITMA RSA

Muhammad Dava D., Adi Fajaryanto C., Moh. Bhanu S.

Program Studi Teknik Informatika, Fakultas Teknik

Universitas Muhammadiyah Ponorogo

Email : muhammadavd4@gmail.com

ABSTRAK

Canggihnya zaman menjadikan informasi sangat tendensi untuk diperhatikan. Cara untuk menanggulangi kepalsuan agar menjaga keaslian dari suatu sertifikat maka dibutuhkan suatu mekanisme yakni dengan pembuatan *digital signature* pada sertifikat. *Digital signature* dibangun dengan memanfaatkan fungsi *hash SHA-256* dan kriptografi algoritma *RSA* (*Rivest Shamir Adleman*). Praktiknya yakni tanda tangan bertipe *file .PNG* dikenakan fungsi *hash SHA-256* sehingga menghasilkan *message digest*, kemudian *message digest* dienkripsi menggunakan kunci pribadi algoritma *RSA* yang telah dibangkitkan untuk mendapatkan *digital signature*. Selanjutnya tahap untuk verifikasi tanda tangan digital dari sertifikat dilakukan dengan mendekripsikan *digital signature* menggunakan kunci publik yang dibongkar oleh kunci privat dari algoritma *RSA*. Ketika pembongkaran kunci maka dilakukan pembandingan, apakah keduanya bernilai sama atau tidak untuk kunci publik dan kunci privat. Dengan penelitian yang dibahas maka akan menghasilkan *digital signature* yang berbeda-beda dari setiap sertifikat dan memiliki evaluasi rata-rata 82,10 Kb/s untuk enkripsi dan 54,60 Kb/s untuk dekripsi.

Kata kunci : Algoritma RSA, Dekripsi, Enkripsi, Sertifikat, *SHA-256*.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakaaatuh.

Puji syukur Alhamdulillah kehadirat Allah SWT dengan ridho dan rahmat-Nya saya mampu menyelesaikan tahap ini tepat pada waktunya. Sholawat serta salam kepada Nabi Muhammad SAW yang telah membawa ummatnya dari zaman kegelapan menuju zaman yang terang benerang penuh dengan ilmu, dan semoga kita semua mendapatkan syafaat di hari akhir. Aamiin.

Skripsi ini jauh dari kata sempurna namun, segala usaha dan do'a telah diikhtiarkan hingga akhirnya saya dapat menyelesaikan pendidikan ini. Segala masukan dan saran akan sangat membantu saya untuk kedepannya dapat menulis dengan lebih baik. Banyak sekali pihak yang telah terlibat, membantu agar skripsi ini menjadi lebih berguna. Untuk itu saya mengucapkan banyak terima kasih kepada :

1. Bapak Edy Kurniawan, S.T., M.T selaku Dekan Fakultas Teknik Universitas Muhammadiyah Ponorogo.
2. Bapak Adi Fajaryanto Cobantoro, S.Kom., M.Kom selaku Kepala Progam Studi Teknik Informatika Universitas Muhammadiyah Ponorogo sekaligus Dosen Pembimbing 1.
3. Bapak Moh. Bhanu Styawan, S.T, M.Kom selaku Dosen Pembimbing 2.
4. Ibu Indah Puji Lestari, S.Kom., M.Kom. dan Ibu Khoiru Nurfitri, S.Kom., M.Kom selaku Dosen Penguji.
5. Teman-teman Program Studi Teknik Informatika angkatan 2018, khususnya kelas D Teknik Informatika serta seluruh teman-teman organisasi sekalian.

Semoga skripsi ini menjadi semangat untuk dapat berkontribusi kepada masyarakat kelak. Segala kesalahan yang tidak sengaja saya lakukan, saya mohon maaf yang sebesar- besarnya.

Wassalamu'alaikum Warahmatullahi Wabarakaaatuh.

DAFTAR ISI

HALAMAN PENGESAHAN	ii
PERNYATAAN ORISINALITAS SKRIPSI	iii
HALAMAN BERITA ACARA UJIAN	iv
BERITA ACARA	v
BIMBINGAN SKRIPSI.....	v
BERITA ACARA	Error! Bookmark not defined.
BIMBINGAN SKRIPSI.....	Error! Bookmark not defined.
SURAT KETERANGAN HASIL PLAGIASI SKRIPSI	x
HALAMAN MOTTO	xii
HALAMAN PERSEMPBAHAN.....	xiii
ABSTRAK	xv
KATA PENGANTAR	xvi
DAFTAR ISI.....	xvii
DAFTAR GAMBAR	xix
DAFTAR TABEL.....	xx
BAB I PENDAHULUAN.....	Error! Bookmark not defined.
1.1 LATAR BELAKANG	Error! Bookmark not defined.
1.2 RUMUSAN MASALAH.....	Error! Bookmark not defined.
1.3 TUJUAN	Error! Bookmark not defined.
1.4 BATASAN MASALAH	Error! Bookmark not defined.
1.5 MANFAAT PENELITIAN.....	Error! Bookmark not defined.
BAB II TINJAUAN PUSTAKA.....	Error! Bookmark not defined.
2.1 TINJAUAN PENELITIAN.....	Error! Bookmark not defined.
2.2 LANDASAN TEORI.....	Error! Bookmark not defined.
2.2.1 PENGERTIAN SERTIFIKAT	Error! Bookmark not defined.
2.2.2 KROPTOGRAFI.....	Error! Bookmark not defined.
2.2.3 TUJUAN KRIPTOGRAFI.....	Error! Bookmark not defined.
2.2.4 SYMMETRIC CRYPTOSISTEM	Error! Bookmark not defined.
2.2.5 ASSYMMETRIC CRYPTOSISTEM	Error! Bookmark not defined.
2.2.6 TANDA TANGAN DIGITAL.....	Error! Bookmark not defined.

- 2.2.7 *SHA-256 (Secure Hash Algoritma)*Error! Bookmark not defined.
- 2.2.8 *ALGORITMA RIVEST SHAMIR ADLEMAN (RSA)* ... Error! Bookmark not defined.
- 2.2.9 *PHP (Personal Hypertext Preprocessor)*Error! Bookmark not defined.
- 2.2.10 *MySQL (My Structure Query Language)*.....Error! Bookmark not defined.

BAB III METODE PENELITIANError! Bookmark not defined.

- 3.1 TAHAP PENELITIANError! Bookmark not defined.
- 3.2 IDENTIFIKASI DAN ANALISA MASALAH....Error! Bookmark not defined.
- 3.2.1 IDENTIFIKASI MASALAH.....Error! Bookmark not defined.
- 3.2.2 ANALISA MASALAHError! Bookmark not defined.
- 3.3 STUDI LITERATUR.....Error! Bookmark not defined.
- 3.4 PENGUMPULAN DATAError! Bookmark not defined.
- 3.5 PERANCANGAN SISTEMError! Bookmark not defined.
- 3.5.1 *QUICK DESIGN (DESAIN CEPAT)*Error! Bookmark not defined.
- 3.6 EVALUASI THROUGHPUT.....Error! Bookmark not defined.

BAB IV HASIL DAN PEMBASANError! Bookmark not defined.

BAB V PENUTUPError! Bookmark not defined.

DAFTAR PUSTAKAError! Bookmark not defined.

DAFTAR GAMBAR

- Gambar 2. 1 Bagan Kriptografi SimetrisError! Bookmark not defined.
- Gambar 2. 2 Bagan Kriptografi AssimetrisError! Bookmark not defined.
- Gambar 2. 3 Skema Digital Signature.....Error! Bookmark not defined.
- Gambar 2. 4 Jalur Komputasi SHA-256Error! Bookmark not defined.
- Gambar 3. 1 Flowchart Tahapan penelitianError! Bookmark not defined.
- Gambar 3. 2 Model WaterfallError! Bookmark not defined.
- Gambar 3. 3 Flowchart pembentuk digital signature dengan Algoritma RSA
.....Error! Bookmark not defined.
- Gambar 3. 4 Flowchart Hash file Ttd .PNGError! Bookmark not defined.
- Gambar 3. 5 Flowchart Proses Enkripsi.....Error! Bookmark not defined.
- Gambar 3. 6 Flowchart Verifikasi atau dekripsiError! Bookmark not defined.
- Gambar 3. 7 Diagram ContextError! Bookmark not defined.
- Gambar 3. 8 DFD pada level 0Error! Bookmark not defined.
- Gambar 3. 9 Entity Relationship Diagram (ERD) .Error! Bookmark not defined.
- Gambar 3. 10 Form Login.....Error! Bookmark not defined.
- Gambar 3. 11 Form HomeError! Bookmark not defined.
- Gambar 3. 12 Penerima.....Error! Bookmark not defined.
- Gambar 3. 13 Upload Tanda tanganError! Bookmark not defined.
- Gambar 3. 14 Penerbitan.....Error! Bookmark not defined.
- Gambar 3. 15 List Sertifikat.....Error! Bookmark not defined.
- Gambar 3. 16 Verifikasi.....Error! Bookmark not defined.

DAFTAR TABEL

- Tabel 2.1 Penelitian Terdahulu **Error! Bookmark not defined.**
- Tabel 2. 2 Value permulaannya Variabel SHA-256 **Error! Bookmark not defined.**
- Tabel 3. 1 User **Error! Bookmark not defined.**
- Tabel 3. 2 Penerima..... **Error! Bookmark not defined.**
- Tabel 3. 3 Digital Signature **Error! Bookmark not defined.**
- Tabel 3. 4 Sertifikat..... **Error! Bookmark not defined.**
- Tabel 3. 5 Verifikasi..... **Error! Bookmark not defined.**
- Tabel 3. 6 Perhitungan besaran file dengan waktu enkripsi & dekripsi..... **Error!**
Bookmark not defined.
- Tabel 4. 1 Percobaan Black Box **Error! Bookmark not defined.**
- Tabel 4. 2 Evaluasi Throughput **Error! Bookmark not defined.**

