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

Muhammad Dava Dharmawan
18532988

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,	Dosen Pembimbing II,
Adi Fajaryanto C., S.Kom., M.Kom	**Moh. Bhanu Setyawan, S.T., M.Kom**
NIK. 19840924 201309 13	NIK. 19800225 201309 13

Mengetahui,

Dekan Fakultas Teknik,	Ketua Program Studi Teknik Informatika,
Edy Kurniawan, S.T.,M.T	**Adi Fajaryanto C., S. Kom., M.Kom**
NIK. 19771026 200810 12	NIK. 19840924 201309 13

ii

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

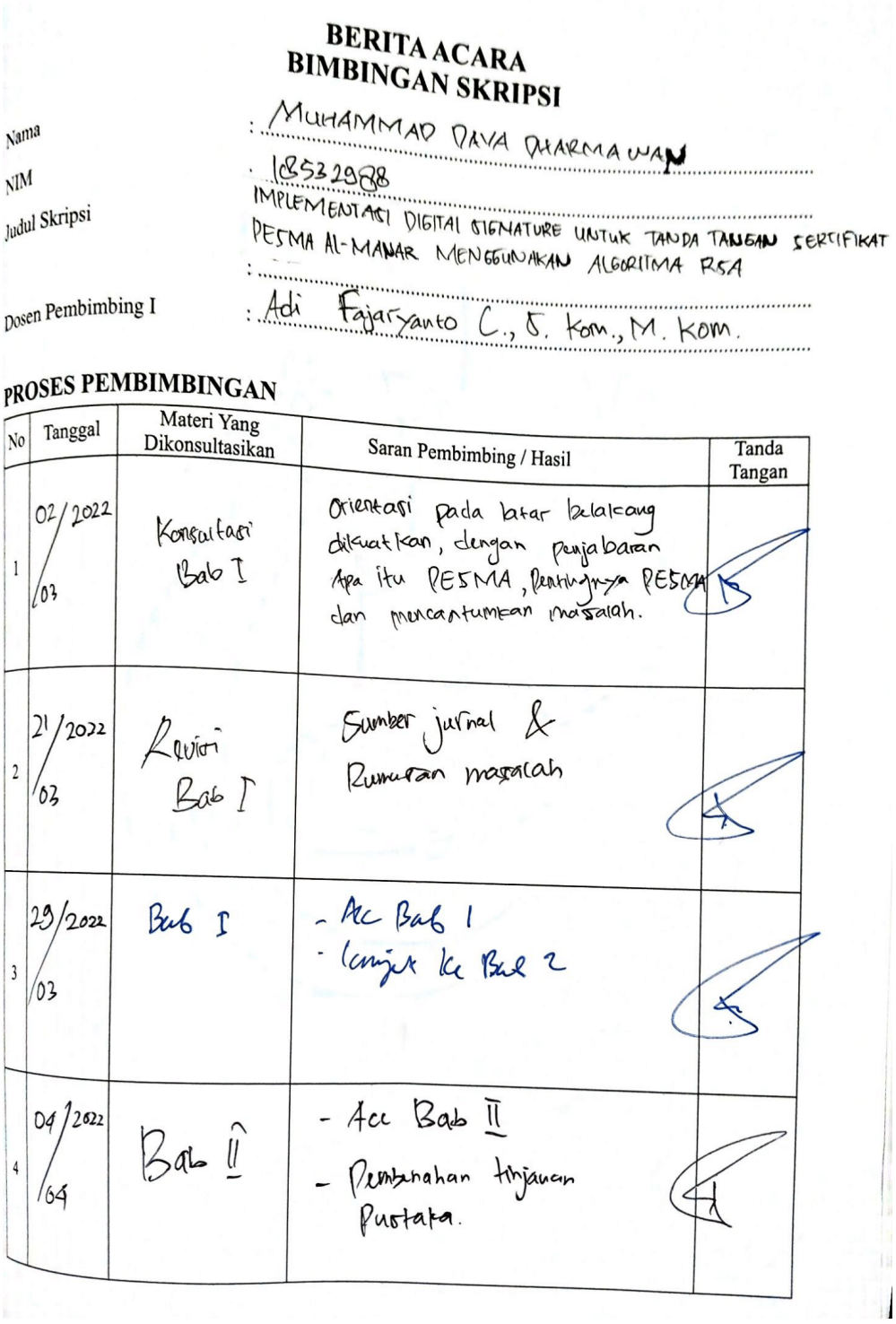
Dosen Penguji,

Dosen Penguji I,	Dosen Penguji II,
Indah Puji Astuti, S.Kom., M.Kom	**Ismail Abdulrazzaq Z., S.Kom, M.Kom**
NIK. 19860424 201609 13	NIK. 19880728 201804 13

Mengetahui,

Dekan Fakultas Teknik,	Ketua Program Studi Teknik Informatika,
Edy Kurniawan, S.T.,M.T	**Adi Fajaryanto C., S. Kom., M.Kom**
NIK. 19771026 200810 12	NIK. 19840924 201309 13

BERITA ACARA
BIMBINGAN SKRIPSI



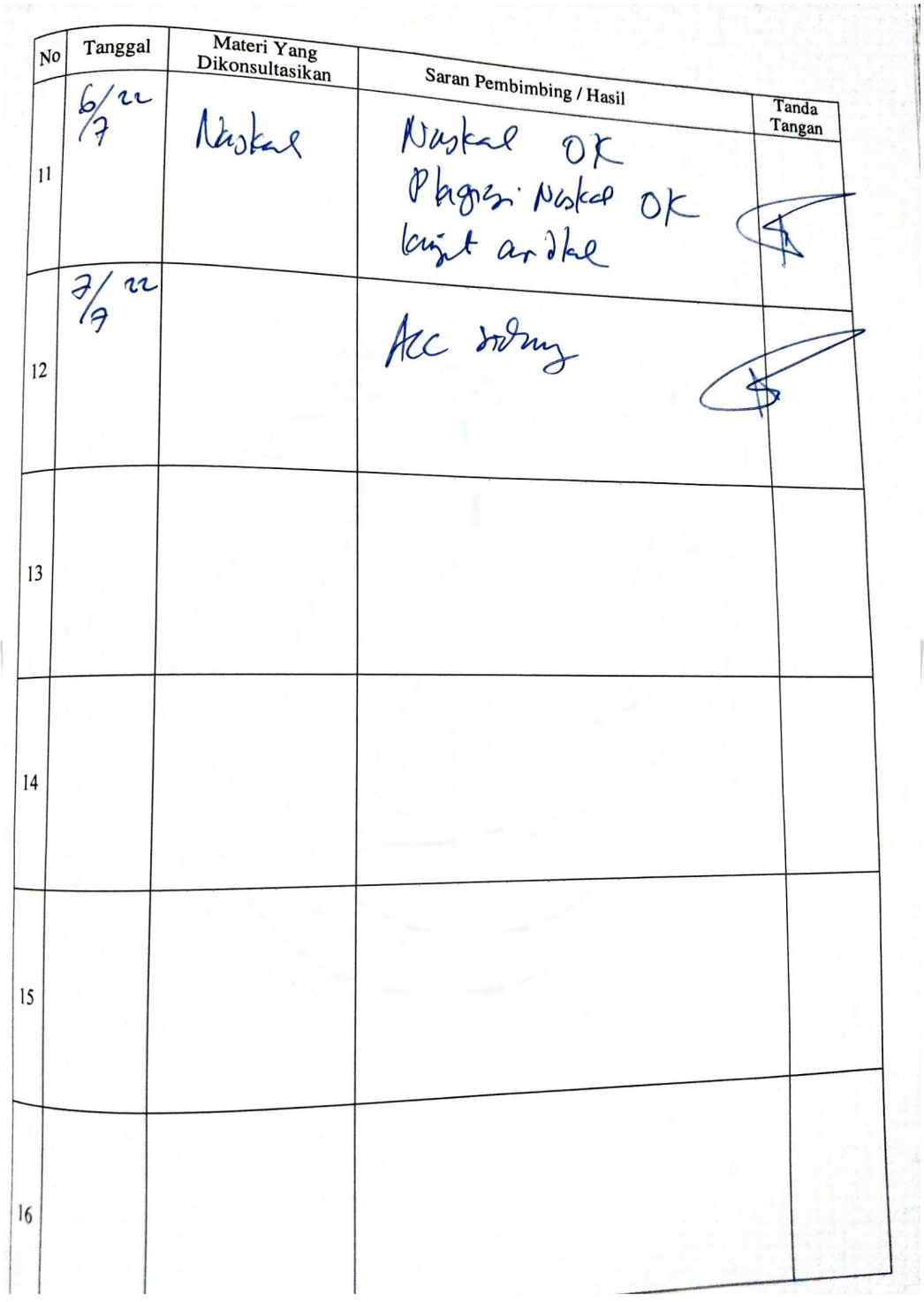
BERITA ACARA
BIMBINGAN SKRIPSI

Nama : MUHAMMAD DAVA DHARMAWAN
NIM : 18532988
Judul Skripsi : IMPLEMENTASI DIGITAL SIGNATURE UNTUK TANDA TANGAN SERTIFIKAT PESMA AL-MANAR MENGGUNAKAN ALGORITMA RSA
Dosen Pembimbing I : 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 latar belakang ditekatkan, dengan penjabaran apa itu PESMA, kenapanya PESMA dan mencantumkan masalah.	
2	21/2022/03	Revisi Bab I	Sumber jurnal & Rumusan masalah	
3	29/2022/03	Bab I	- Acc Bab I - Lanjut ke Bab 2	
4	04/2022/04	Bab II	- Acc Bab II - Perbanahan tinjauan Pustaka.	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
5	05/2022 09	Bab 3	Melihat penulisan para: prototype , hasil flowchart ditambah deskripsinya	
6	12/22 4	Bab 3	tambahkan Relasi tabel. flowchart & Kamus tabel	
7	19/22 4	Proposal	Acc Seminar Proposal	
8	03/22 05	Revisi Project	Terkait disederhanakan untuk gambar & teks hasilnya dgn Verifikasi	
9	19/22 05	Penerapan Bab IV	Lanjut naskah bab IV Serta Penambahan Saran.	
10	27/22 6	Naskah	- Kritis artikel - cek plagiasi.	



No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
11	6/7 22	Naskah	Naskah OK Plagasi Naskah OK kirim artikel	
12	7/7 22		Acc sidang	
13				
14				
15				
16				

BERITA ACARA
BIMBINGAN SKRIPSI

Nama : MUHAMMAD DAVA DHARMAWAN.

NIM : 18532988

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

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

PROSES PEMBIMBINGAN

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
1	02/2022 /03	Konsutasi Judul	Cari banyak Referensi.	
2	30/2022 /03	Revisi Bab I	Landasan sertifikat elektronik Cari Referensinya.	
3	05/2022 /04	Acc Bab I Revisi Bab II Revisi Bab III	Bab II kasih perbedaan didalam Tabel penelitian. Bab III kasih evaluasinya.	
4	21/2022 /04	Proporal	Acc Seminar Proporal.	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
5	15/06/22	Uji coba Aplikasi	Progres 85 % perbaiki dari hasil revisi	
6	16/06/22	Bab 4	- Data hasil uji coba di perbanyak	
7	02/07/22	Aplikasi	Aplikasi sudah Ok	
8	03/07/22	Bab 5	kesimpulan diambil berdasarkan hasil bab 4 di sinkron dg latar belakang	
9	07/07/22	All	Acc sidang	
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 *SIMILIARITY 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 *SIMILIARITY 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 : muhammaddavad4@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 siganture* 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 Wabarakaatuh.

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 Wabarakaatuh.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL