SKRIPSI

PENERAPAN DIGITAL SIGNATURE DENGAN ALGORTIMA RSA UNTUK MENENTUKAN KEABSAHAN DOKUMEN PENGESAHAN LAPORAN KKP (STUDI KASUS FAKULTAS TEKNIK UNIVERSITAS PELITA BANGSA)

Diajukan untuk memenuhi salah satu syarat
memperoleh Gelar Sarjana Komputer

Disusun oleh:

Sarikhin

311710871

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS PELITA BANGSA

BEKASI

2021

HALAMAN PERSETUJUAN SKRIPSI

PENERAPAN DIGITAL SIGNATURE DENGAN ALGORTIMA RSA UNTUK MENENTUKAN KEABSAHAN DOKUMEN PENGESAHAN LAPORAN KKP (STUDI KASUS FAKULTAS TEKNIK UNIVERSITAS PELITA BANGSA)

Disusun oleh:

Sarikhin

311710871

Telah diperiksa dan dishakan

pada tanggal : ……..

Dosen Pembimbing I	Dosen Pembimbing II
Wahyu Hadikristanto, S.Kom., M.Kom	**Bambang Hermanto, S,E, M.Kom**
NIDN.	**NIDN.**

Mengetahui,

Ketua Program Studi Teknik Informatika

Aswan Supriyadi Suge, S.E, M.Kom

NIDN. 04260108003

LEMBAR PENGESAHAN

PENERAPAN DIGITAL SIGNATURE DENGAN ALGORTIMA RSA UNTUK MENENTUKAN KEABSAHAN DOKUMEN PENGESAHAN LAPORAN KKP

Disusun oleh:

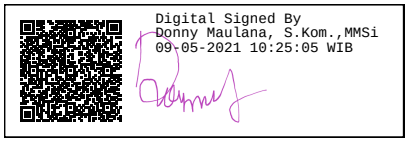
Sarikhin

311710871

Telah dipertahankan didepan Dewan Penguji

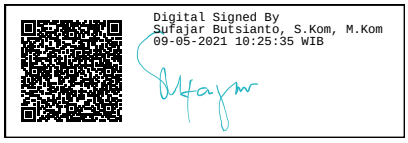
pada tanggal : ……..

Dosen Penguji I



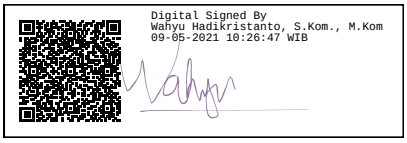
Donny Maulana, S.Kom.,MMSi
NIDN.

Dosen Penguji II



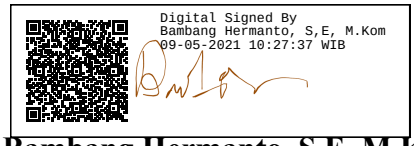
Sufajar Butsianto, S.Kom, M.Kom
NIDN.

Dosen Pembimbing I



Wahyu Hadikristanto, S.Kom., M.Kom
NIDN.

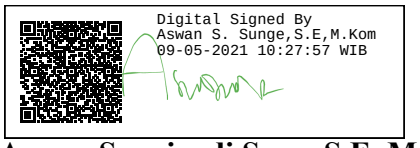
Dosen Pembimbing II



Bambang Hermanto, S,E, M.Kom
NIDN.

Mengetahui,

Ketua Program Studi Teknik Informatika



Aswan Supriyadi Suge, S.E, M.Kom
NIDN. 04260108003

Dekan Fakultas Teknik

Putri Anggun Sari, S.Pt., M.Si.

NIDN. 0424088403

PERNYATAAN
KEASLIAN SKRIPSI

Sebagai mahasiswa Universitas Pelita Bangsa, yang bertanda tangan dibawah ini, saya:

Nama : Sarikhin
NIM : 311710871

Menyatakan bahwa karya ilmiah yang berjudul:

"Penerapan Digital Signature Dengan Algortima RSA Untuk Menentukan Keabsahan Dokumen Pengesahan Laporan KKP"

merupakan karya asli saya(kecuali cuplikan dan ringkasan yang masing-masing telah saya jelaskan sumbernya dan perangkat pendukung). Apabila dikemudian hari, karya saya disinyalir bukan merupakan karya asli saya, yang disertai dengan bukti-bukti yang cukup, maka saya bersedia untuk membatalkan gelar saya berserta hak dan kewajiban yang melekat pada gelar tersebut. Demikian surat pernyataan ini saya buat dengan sebenarnya.

Dibuat : Bekasi
Pada Tanggal : 16 April 2021

Yang Menyatakan,

Sarikhin

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai mahasiswa Universitas Pelita Bangsa, yang bertanda tangan dibawah ini, saya :

Nama : Sarikhin

NIM : 311710871

demi mengembangkan Ilmu Pengetahuan, menyetujui untuk memberikan kepada Universitas Pelita Bangsa Hak Bebas Royalti Non-Elsklusif (*Non Exclusive Royalty Free Right)* atas karya ilmiah yang berjudul :

"Penerapan Digital Signature Dengan Algortima RSA Untuk Menentukan Keabsahan Dokumen Pengesahan Laporan KKP"

Beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Elsklusif ini Universitas Pelita Bangsa berhak unuk menyimpan, mengcopy ulang (memperbanyak), menggunakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikan dan menampilkan/mempublikasikannya diinternet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Universitas Pelita Bangsa segala bentuk tuntutan hukum yang timbul atau pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

Dibuat : Bekasi

Pada Tanggal : 16 April 2021

Yang Menyatakan,

Sarikhin

BAB 1
PENDAHULUAN

1. Latar Belakang Masalah

Dengan adanya pandemi Covid-19 seperti saat ini, mengharuskan masyarakat untuk membatasi kerumunan. Hal ini mengakibatkan banyak berubahan aktifitas pada masyarakat, salah satu nya aktifitas belajar mengajar dilakukan melalui daring. Dengan tidak adanya aktifitas belajar dan mengajar secara tatap muka berdampak juga dengan sulitnya untuk mendapatkan tanda tangan pada lembar pengesalah laporan KKP. Untuk saat ini solusinya adalah dengan membubuhkan tanda tangan pada *soft* dokumen dan merubahnya menjadi bentuk file PDF. Akan tetapi solusi tersebut bukanlah solusi yang paling tepat, karna terdapat banyak resiko yang dapat terjadi seperti pemalsuan tanda tangan. Hal tersebut menimbulkan keraguan akan keaslian tanda tangan di setiap lembar pengesahan yang ada.

Masalah keaslian tanda tangan menjadi poin penting, mengingat mudahnya suatu tanda tangan dalam suatu dokumen dapat dimanipulasi dengan sangat mudah dan sulit untuk membedakan antara tanda tangan asli dengan tanda tangan palsu. Pemalsuan tanda tangan ini masih bisa dilakukan karena belum adanya prosedur yang dapat menunjukkan keabsahan tanda tangan pada Universitas Pelita Bangsa.

Berdasar permasalahan keabsahan tanda tangan pada lembar pengesahan diatas, mucullah ide untuk membuat sistem sebagai wadah atau saran dalam memberi tanda tangan pada lembar tersebut. Tanda tangan yang dimaksud adalah tanda tangan digital (*digital signature)* yang bertujuan sebagai upaya untuk menjaga keabsahan suatu dokumen. *Digital Signature* adalah salah satu mekanisme untuk menggantikan tanda tangan secara manual pada dokumen kertas. *Digital Signature* memiliki fungsi sebagai penanda pada data yang dapat memastikan bahwa data tersebut adalah data

yang sebenarnya. Penanda pada *Digital Signature* ini tidak semata hanya berupa tanda tangan digital, tetapi dapat berupa cap *digital, text*, bit, dan gambar. Sistem ini sekaligus dapat melakukan verifikasi terhadap dokumen yang ada apakah dokumen tersebut dalam keadaan asli atau sudah mengalami modifikasi.

2. Identifikasi Masalah

Identifikasi masalah pada penelitian ini adalah :

a. Penentuan keaslian suatu dokumen masih sulit dilakukan karena belum adanya prosedur untuk membuktikan keaslian suatu tanda tangan pada lembar persetujuan Laporan KKP.
b. Permintaan untuk menandatangai lembar persetujuan Laporan KKP menjadi sulit karena belum tersedianya wadah yang digunakan untuk menandatangani dokumen tersebut.
c. Suatu tantangan untuk menjaga keaslian suatu tanda tangan karena mudahnya memanipulasi tanda tangan.

3. Batasan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, penelitian ini berfokus pada proses penandatanganan lembar persetujuan Laporan KKP dari manual ke komputerisasi dengan menerapkan *Digital Signature* pada lembar tersebut.

4. Rumusan Masalah

Rumusan Masalah pada penelitian ini adalah :

a. Bagaimana menjaga keaslian suatu dokumen dengan menggunakan *Digital Signature.*
b. Bagaimana tahapan penggunaan *Digital Signature.*
c. Apakah penggunaan sistem dapat menjadi solusi dengan masalah yang ada.

5. Tujuan penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah :

a. Membuat sistem yang dapat menjadi solusi dari permasalahan yang ada.
b. Menjadikan dokumen dapat di percayai keasliannya

6. Manfaat penelitian

Manfaat yang diharapakan dari penelitian ini adalah :

a. Masalah manipulasi menjadi tidak ada karena sudah terdapat sistem yang dapat mendeteksi keaslian suatu tanda tangan
b. Proses penandatanganan dokumen menjadi lebih mudah

BAB II
TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1. Tinjauan Pustaka

Barbagai penelitian tentang tanda tangan digital telah dibuat sebelumnya. Jurnal dan penelitian yang membahas kemiripan teori maupun subjek penelitian dijadikan sebagai acuan dalam penelitian ini. Berikut merupakan penelitian terdahulu yang membahas tanda tangan digital :

Pertama, penelitian yang dilakukan oleh Leonardo Refialy, Eko Sediyono dan Adi Setiawan (2015) dalam jurnal Teknik Informatika dan Sistem Informasi Volume 1. Mereka meneliti tentang Pengamanan Sertifikat Tanah Digital Menggunakan Digital Signature SHA-512 dan RSA

Pada penelitian ini fungsi *hash* yang digunakan adalah SHA-512 sebagai algoritma tanda tangan digital karena mempunyai waktu paling tepat dan baik dalam melalukan otentikasi. Hasil dari penelitian ini yaitu dapat mengidentifikasi ada tidaknya perubahan pada dokumen yang telah diberi tanda tangan digital sehingga dapat mengetahui adanya proses manipulasi pada dokumen tersebut, serta tidak terjadinya perubahan yang signifikan terhadap *file* dokumen yang belum di beri tanda tangan digital dan telah diberi sehingga secara kasat mata kedua *file* terlihat sama. Selanjutnya sistem yang dihasilkan dari penelitian ini berupa program *desktop* yang hanya dapat diakses menggunakan komputer atau laptop.

Persamaan penelitian sebelumnya dengan penelitian ini adalah sama-sama menggunakan RSA sebagai algoritma enskripsi *public key*. Perbedaan penelitian yang dilakukan terletak pada implementasi sistem dan objek yang digunakan serta algoritma *hash* yang digunakan.

Kedua, penelitian yang dilakukan oleh Egi Cahyo Prabowo dan Irawan Alfrianto (2017) dalam jurnal Ilmiah Komputer dan Informatika (KOMPUTA)

Volume 6. Mereka meneliti tentang Penerapan Digital Signature dan Kriptografi pada Otentikasi Sertifikat Tanah Digital.

Pada penelitian ini fungsi *hash* yang digunakan adalah algoritma SHA-256 dan RSA. SHA-256 dipilih dengan alas an sampai saat ini belum ada yang dapat memecahkan algoritma tersebut dan RSA dipilih karena merupakan sistem pertama yang sekaligus dapat digunakan untuk *key distribution, confidentiality* dan *digital signature.* Hasil dari penelitian ini dapat disimpulkan bahwa penerapan mekanisme pembuatan dokumen digital didalam sistem dapat memberikan layanan alternatif untuk menertibkan dokumen digital dan dapat memberikan layanan keamanan berupa otentikasi dokumen yang diterpakan pada dokumen digital pemohon oleh kepala kantor sehingga pemohon dapat mengetahui validitas dokumen yang diterima.

Persamaan penelitian sebelumnya dengan penelitian ini adalah sama-sama menggunakan algoritma *hash* SHA-256 dan RSA sebagai algortma enkripsi tanda tangan digital. Perbedaan penelitian dilakukan terletak pada implementasi sistem dan objek yang digunakan.

Ketiga, penelitian yang dilakukan oleh Sugiyanto dan Prima Dina Atika (2018) dalam jurnal Cendikia Volume. XVI 2018 yang berjudul Digital Signature dengan Algoritma SHA-1 dan RSA sebagai Autentikasi.

Pada penelitian ini fungsi *hash* yang digunakan adalah SHA-1 karena mempunyai nilai *hash* yang paling kecil. Hasil dari penelitian ini bahwa algoritma *hashing* SHA-1 dan algoritma kriptograpi *Rivest Shamir Adleman* (RSA) dapat dikombinasikan dengan baik dalam membuat sebuah *digital signature* pada file pdf dan aplikasi yang dibuat terbukti mampi diandalkan dalam autentikasi file pdf SKPI dari tindak pemalsuan dan modifikasi data serta aplikasi dapat membantu pihak instansi / perusahaan dari rasa khawatir akan modifikasi atau pemalsuan data Surat Keterangan Pendamping Ijasah (SKPI)

Parsamaan sebelumnya dengan penelitian ini dengan adalah sama menggunakan media *website* sebagai implementasi sistem dan objek yang

sama yaitu dokumen pdf. Perbedaan penelitian terletak pada algoritma *hashing* yang digunakan.

2.2. Landasan Teori

2.2.1. Kriptografi

2.2.1.1.Macam-Macam Kriptografi

2.2.2. Digital Signature

2.2.3. Algortima Rives Shamir Adleman (RSA)

2.2.4. Secure Hashing Algorithm (SHA)

2.2.5. X.509 Certificate

2.2.6. Lembar Pengesahan

2.2.7. Dokumen PDF (Portable Dokumen File)

2.2.8. Bahasa Pemprograman Python

2.2.9. Framework Flask

2.2.10. Library Python Chryptography

2.2.11. Library PyHanko

2.2.12.