

**IMPLEMENTASI ALGORITMA DSA (*DIGITAL SIGNATURE  
ALGORITHM*) DALAM PENGAMANAN DOKUMEN DIGITAL**

**SKRIPSI**

**Oleh**

**ANNISAH AMALIA**

71210915009



**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS ISLAM SUMATERA UTARA**

**2025**

## DAFTAR ISI

<b>KATA PENGANTAR</b>	<b>i</b>
<b>ABSTRAK</b>	<b>iii</b>
<b>DAFTAR ISI</b>	<b>iv</b>
<b>DAFTAR TABEL</b>	<b>vi</b>
<b>DAFTAR GAMBAR</b>	<b>vii</b>
<b>DAFTAR LAMPIRAN</b>	<b>viii</b>
<b>BAB I PENDAHULUAN</b>	<b>1</b>
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Metodologi Penelitian	4
1.7 Sistematika Penulisan	4
<b>BAB II TINJAUAN PUSTAKA</b>	<b>7</b>
2.1 Kriptografi	7
2.1.1 Enkripsi dan Dekripsi	7
2.2 Validasi	8
2.3 Dokumen	8
2.4 <i>Flowchart</i>	9
2.5 Bahasa pemograman <i>python</i>	11
2.6 <i>QR-Code</i>	12
2.7 Dokumen Digital	13

2.8	<i>Digital signature</i>	13
2.9	DSA ( <i>Digital Signature Algorithm</i> )	13
2.8.1	Tujuan DSA ( <i>Digital Signature Algorithm</i> )	14
2.8.2	Keunggulan Dan Kekurangan DSA ( <i>Digital Signature Algorithm</i> )	14
2.9	Penelitian Terdahulu	16
<b>BAB III METODE PENELITIAN</b>		<b>18</b>
3.1	Peralatan Pendukung	18
3.1.1	Perangkat Keras	18
3.1.2	Perangkat Lunak	18
3.2	Metode Pengumpulan Data	19
3.3	<i>Flowchart</i>	19
3.3.1	<i>Flowchart</i> Aplikasi	19
3.3.2	<i>Flowchart</i> Kerangka Kerja	20
3.4	Perhitungan DSA ( <i>Digital Signature Algorithm</i> )	21
3.5	Rancangan Antar Muka Aplikasi	24
<b>BAB IV HASIL DAN PEMBAHASAN</b>		<b>26</b>
4.1	Implementasi Aplikasi	26
4.1.1	Tampilan Aplikasi	26
4.2	Pengujian Aplikasi	31
<b>BAB V KESIMPULAN DAN SARAN</b>		<b>33</b>
5.1	Kesimpulan	33
5.2	Saran	33
<b>DAFTAR PUSTAKA</b>		<b>34</b>

## DAFTAR TABEL

<b>Tabel 2.1</b> Arti simbol <i>flowchart</i>	9
<b>Tabel 3.1</b> Kebutuhan perangkat keras	18
<b>Tabel 3.2</b> Kebutuhan perangkat lunak	18

## DAFTAR GAMBAR

<b>Gambar 2.1</b> Contoh gambar <i>QR-Code</i>	12
<b>Gambar 3.1</b> <i>Flowchart</i> aplikasi	19
<b>Gambar 3.2</b> <i>Flowchart</i> kerangka kerja	20
<b>Gambar 3.3</b> Rancangan antarmuka aplikasi	24
<b>Gambar 4.1</b> Tampilan aplikasi	26
<b>Gambar 4.2</b> Tampilan <i>signer name</i>	27
<b>Gambar 4.3</b> Tampilan <i>sign document</i>	28
<b>Gambar 4.4</b> Tampilan <i>verify signature</i>	29
<b>Gambar 4.5</b> Tampilan <i>generate QR-Code &amp; Add to Document</i>	30
<b>Gambar 4.6</b> Tampilan dokumen yang sudah ditandatangani	31
<b>Gambar 4.7</b> Tampilan hasil <i>scan QR-Code</i>	32

## DAFTAR LAMPIRAN

	Halaman
Surat Ketetapan Pembimbing	L-1
Kartu Bimbingan Dosen Pembimbing I	L-2
Kartu Bimbingan Dosen Pembimbing II	L-3

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Tandatangan adalah suatu bentuk representasi identitas seseorang yang biasanya ditulis dengan tangan dan digunakan untuk mengesahkan dokumen atau menyatakan persetujuan. Tandatangan sering kali berupa nama atau simbol khas yang ditulis oleh individu. Secara legal, tandatangan memiliki fungsi penting dalam mengakui atau menyetujui kontrak, surat pernyataan, atau dokumen resmi lainnya (Lapian et al. 2024).

*Digital Signature* atau tandatangan digital adalah mekanisme kriptografi yang digunakan untuk memberikan jaminan keaslian dan integritas data dalam transaksi elektronik. Tandatangan digital memastikan bahwa pesan atau dokumen yang ditandatangani berasal dari sumber yang valid (otentik) dan tidak diubah sejak ditandatangani (integritas) (Ramdan 2024).

Untuk mengatasi resiko modifikasi atau pemalsuan dokumen digital, diperlukan suatu teknik keamanan dokumen digital. Salah satu cara efektif adalah dengan memberikan tandatangan digital.

*Digital signature* bukanlah tandatangan manual yang di digitalkan, melainkan sebuah pengkodean yang di dapat dari proses *Digital Signature Algorithm* (DSA). DSA menggunakan kunci publik dan kunci privat untuk membuat dan memverifikasi tandatangan digital.

Permasalahan utama pada penelitian ini tentang keamanan, pemilihan kunci DSA memerlukan dua bilangan prima yang besar untuk pembangkitan kunci. Keamanan DSA bergantung pada kerahasiaan kunci privat. Jika kunci privat

## DAFTAR PUSTAKA

- Ajhari, Abdul Azzam, and Windarto Windarto. 2018. "Implementasi Algoritma Affine Cipher Dan Aes-128 Untuk Pengamanan Pesan Dan One Time Password Registrasi Akun Pada Aplikasi Chatting Berbasis Android Di Sma Hang Tuah 1 Jakarta." *Skanika* 1(1):323–34.
- Alfani, Mhd Reza, Mhd Furqan, and Yusuf Ramadhan Nasution. 2024. "Pengamanan Data Teks Menggunakan Metode Digital Signature Algorithm (Dsa) Dan Advanced Encryption Standard (Aes)." *Journal of Science and Social Research* 4307(1):301–6.
- Alwan, Dhana Arvina, and Nurul Qomariasih. 2024. "Penerapan Tanda Tangan Digital Dan Secure Coding Berdasarkan OWASP Pada Sistem E-Control Tugas Akhir." *Info Kripto* 18(2):49–55. doi: 10.56706/ik.v18i2.100.
- Azhari, Muhammad, Dadang Iskandar Mulyana, Faizal Joko Perwitosari, and Firhan Ali. 2022. "Implementasi Pengamanan Data Pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)." *Jurnal Pendidikan Sains Dan Komputer* 2(01):163–71. doi: 10.47709/jpsk.v2i01.1390.
- Eritza, Afnita, Mukhlis Ramadhan, and Hafizah Hafizah. 2022. "Penerapan Digital Signature Metode SHA Dan Contoh Perhitungan DSA." *Jurnal Sistem Informasi Triguna Dharma (JURSI TGD)* 1(6):906. doi: 10.53513/jursi.v1i6.6002.
- Hermawan, Latius, and Maria Bellaniar Ismiati. 2020. "Aplikasi Pengecekan

Dokumen Digital Tugas Mahasiswa Berbasis Website.” *Jurnal Buana Informatika* 11(2):94–103. doi: 10.24002/jbi.v11i2.3706.

Lapian, Randy, Deasy Soeikromo, and Rudolf S. Mamengko. 2024. “PENGATURAN PENGGUNAAN TANDA TANGAN ELEKTRONIK MENURUT UU NO. 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK.” *Lex Privatum* 13(1).

M.Miftakul, Amin. 2016. “IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS.” *Jurnal Pseudocode* III(September):129–36.

Muharram, Faturungi, Huzain Azis, and Abdul Rachman Manga. 2018. “Analisis Algoritma Pada Proses Enkripsi Dan Dekripsi File Menggunakan Advanced Encryption Standard (AES).” *Prosiding Seminar Nasional Ilmu Komputer Dan Teknologi Informasi* 3(2):112–15.

Musthofa, Novan Adi, Siti Mutrofin, and Mohamad Ali Murtadho. 2016. “IMPLEMENTASI QUICK RESPONSE ( QR ) CODE PADA APLIKASI VALIDASI DOKUMEN MENGGUNAKAN PERANCANGAN UNIFIED MODELLING LANGUAGE ( UML ).” 10(1):42–50.

Nugrohadhi, Agung. 2015. “Pengorganisasian Dokumen Dalam Kegiatan Kepustakawanan.” *Khizanah Al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan* 3(1):1–10. doi: 10.24252/kah.v3i1a1.

P. Rosyani, A. Riski, FF. Gism. Ripan. 2023. “BAHASA PEMROGRAMAN PYTHON.” 1(1):46–49.

- Pardosi, Irpan Adiputra, and Ronsen Purba. 2015. "PEMERIKSAAN INTEGRITAS DOKUMEN DENGAN DIGITAL SIGNATURE ALGORITHM." *Jurnal SIFO Mikroskil* 16(1):73–82. doi: 10.55601/jsm.v16i1.180.
- Permana, Angga Aditya. 2019. "Pengamanan Teks Menggunakan Metode Algoritma Rsa Dengan Verifikasi Realtime Biometrik Menggunakan Opencv." *Jurnal Teknik* 7(2). doi: 10.31000/jt.v7i2.1352.
- Ramdan, M. Fairuz. 2024. "Studi Perbandingan Teknik Thresholding Untuk Binarisasi Tanda Tangan Menggunakan OpenCV2: Metode Sederhana, Adaptif, Dan Otsu." 2(2):166–72.
- Rehulina, Rehulina. 2018. "Keabsahan Digital Signature Dalam Perjanjian E-Commerce." *Doktrina: Journal of Law* 1(1):45. doi: 10.31289/doktrina.v1i1.1609.
- Rochman, Fatich Fazlur. 2016. "Implementasi QR Code Dan Digital Signature Untuk Menentukan Keabsahan Dokumen Krs Dan Khs (Studi Kasus Fakultas Sains Dan Teknologi Universitas Airlangga)."
- Rosaly, Rizqi, and Andy Prasetyo. 2020. "Flowchart Beserta Fungsi Dan Simbol-Simbol." *Journal of Chemical Information and Modeling* 2(3):5–7.
- Sarjana, Program Pasca, and Universitas Diponegoro. 2011. "E-Dokumen Dengan Metode Hybrid : Biometrik Tandatangan Dan Dsa ( Digital Signature Algorithm )." 1–150.
- Taqiyyah, Rufaidah, and Ahmad Rio Adriansyah. 2020. "Implementasi Fungsi

Hash Untuk Otentikasi File Digital (Digital Signature).” *Jurnal Informatika Terpadu* 6(1):07–13. doi: 10.54914/jit.v6i1.213.

Yuniati, Trihastuti, and Muhammad Fajar Sidiq. 2020. “Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital Sebagai Alternatif Pengesahan Dokumen Di Masa Pandemi.” *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)* 4(6). doi: 10.29207/resti.v4i6.2502.



الجامعة الإسلامية في سومطرة الشمالية  
UNIVERSITAS ISLAM SUMATERA UTARA  
FAKULTAS TEKNIK  
**PROGRAM STUDI TEKNIK INFORMATIKA**  
JL. S. M. RAJA TELP. : (061) 7868049 FAX. : (061) 7868049 TELADAN MEDAN KODE POS 20217  
www.ft.uisu.ac.id

**SURAT-KEPUTUSAN**  
Nomor : 53/UISU/FT-KPSTIK/X/2024

**Tentang**  
**TUGAS SKRIPSI MAHASISWA**

Memperhatikan : 1. Kemajuan studi mahasiswa

**Nama : ANISAH AMALIA**  
**NPM : 71210915009**

telah menyelesaikan sebagian besar tugas-tugas/mata kuliah pada kurikulum Program Studi Teknik Informatika Fakultas Teknik UISU Medan, kecuali Tugas Skripsi mahasiswa.

2. Telah disetujuinya mahasiswa pada butir (1) untuk melaksanakan Tugas Skripsi mahasiswa, dengan judul skripsi :  
**“ Implementasi Algoritma DSA (Digital Signature Algorithm) Dalam Pengamanan Dokumen Digital ”**
3. Surat Permohonan Pembimbing Skripsi mahasiswa pada butir (1) diatas.  
Bahwa perlu menetapkan dan mengangkat pembimbing untuk mahasiswa pada butir (1) dalam menyelesaikan Tugas Skripsi nya.

**MEMUTUSKAN**

- Menetapkan :
1. Merekomendasikan kepada mahasiswa pada butir (1) diatas untuk melaksanakan Tugas Skripsi.
  2. Dosen Pembimbing untuk mahasiswa pada butir (1) adalah sebagai berikut :
    - a. Pembimbing I : **Mhd. Zulfansyuri Siambaton, ST, M.Kom**
    - b. Pembimbing II: **Tasliyah Haramaini, S.Si, M.Kom**
  3. Surat Keputusan ini diberikan kepada yang bersangkutan untuk dilaksanakan sebaik-baiknya dan berlaku mulai tanggal **01 Oktober 2024 s/d 01 April 2025**.
  4. Bilamana dikemudian hari ternyata ada kekeliruan dalam penetapan ini, akan diperbaiki sebagaimana mestinya.

Ditetapkan: **Medan**  
Pada Tanggal: **01 Oktober 2024**

Ketua Program Studi,



**Mhd. Zulfansyuri Siambaton, ST, M.Kom**  
NIDN. 0103098503

**Tembusan:**

1. Dosen Pembimbing
2. Mahasiswa Ybs.
3. Peringgal

**KARTU BIMBINGAN SKRIPSI**

NAMA : ANNISAH AMALIA  
NPM : 71210915009  
JUDUL : IMPELEMENTASI ALGORITMA DSA (DIGITAL SIGNATURE ALGORITHM) DALAM PENGAMANAN DOKUMEN DIGITAL  
DOSEN PEMBIMBING : MHD. ZULFANSYURI SIAMBATON, ST, M.KOM









NO	HARI / TANGGAL	CATATAN	PARAF PEMBIMBING
1	Senin/30-09-24	Acc Judul Laporan Skripsi	[Signature]
2	Rabu/02-10-24	Bab I: Perbaiki Bab II Belakang, RMBing. Bab II: Tambahkan literatur yg terkait.	[Signature]
3	Rabu/09-10-24	Bab I & II OK, lanjut Bab III & IV	[Signature]
4	Kamis/17-10-24	Bab III: Perbaiki Gambar Tanpa Desain. Bab IV: Perbaiki Program Aplikasi	[Signature]
5	Jumat/25-10-24	Bab III & IV OK, lanjut Bab V	[Signature]
6	Senin/4-11-24	Bab V perbaiki kesimpulan.	[Signature]
7	Jumat/08-11-24	Bab V OK, lengkapi Skripsi	[Signature]
8	Senin/11-11-24	Acc Seminar Hasil	[Signature]
9			
10			

Medan, 11 Nopember 2024  
Menyetujui,  
Dosen Pembimbing

(Mhd. Zulfansyuri Siambaton, ST., M.Kom)

### KARTU BIMBINGAN SKRIPSI

NAMA : ANNISAH AMALIA  
NPM : 71210915009  
JUDUL : IMPELEMENTASI ALGORITMA DSA (DIGITAL SIGNATURE ALGORITHM) DALAM PENGAMANAN DOKUMEN DIGITAL  
DOSEN PEMBIMBING : TASLIYAH HARAMAINI, S.SI., M.KOM

NO	HARI / TANGGAL	CATATAN	PARAF PEMBIMBING
1	Jum'at 18 Okt 2024	Revisi Bab I, batasan masalah, sistematika	
2	Jenin 28 Okt. '24	Acc Bab I, Revisi Bab II	
3	Kamis/ 31 Okt. '24	Acc Bab II	
4	Rabu/ 6 Nov. '24	Revisi Bab III, Bab IV	
5	Jum'at/ 8 Nov. '24	Acc Bab III, Bab IV	
6	Jenin/ 11 Nov. '24	Revisi Bab V, D. pustaka	
7	Kamis/ 14 Nov. '24	Acc Bab V & D. pustaka	
8	Sabtu/ 16 Nov '24	Running Program Acc	
9			
10			

Medan, 16 Nopember 2024  
Menyetujui,  
Dosen Pembimbing



(Tasliyah Haramaini, S.Si., M.Kom)