

**IMPLEMENTASI *DIGITAL SIGNATURE ALGORITHM* (DSA)  
MENGUNAKAN *SECURE HASH ALGORITHM-256* (SHA-256)  
PADA MEDIA GAMBAR**

**Skripsi**

diajukan untuk memenuhi sebagian syarat untuk memperoleh  
Gelar Sarjana Matematika



Oleh :  
Sahl Fawzy Sutopo  
1603926

**DEPARTEMEN PENDIDIKAN MATEMATIKA  
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
UNIVERSITAS PENDIDIKAN INDONESIA  
2020**

**IMPLEMENTASI *DIGITAL SIGNATURE ALGORITHM* (DSA)  
MENGUNAKAN *SECURE HASH ALGORITHM-256* (SHA-256)  
PADA MEDIA GAMBAR**

Oleh  
Sahl Fawzy Sutopo  
NIM. 1603926

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

© Sahl Fawzy Sutopo  
Universitas Pendidikan Indonesia  
September 2020

© Hak Cipta dilindungi undang-undang.

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,  
dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari penulis.

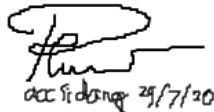
**LEMBAR PENGESAHAN**

SAHL FAWZY SUTOPO

IMPLEMENTASI *DIGITAL SIGNATURE ALGORITHM* (DSA)  
MENGUNAKAN *SECURE HASH ALGORITHM-256* (SHA-256)  
PADA MEDIA GAMBAR

Disetujui dan disahkan oleh pembimbing:

Pembimbing I



acc si desng 29/7/20

**Dra. Hj. Rini Marwati, M.S.**

**NIP. 196606251990012001**

Pembimbing II

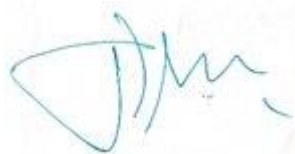


**Dr. H. Cece Kustiawan, M.Si.**

**NIP. 196612131992031001**

Mengetahui,

Ketua Departemen Pendidikan Matematika,



**Dr. H. Dadang Juandi, M.Si.**

**NIP. 196401171992021001**

## ABSTRAK

Dengan berkembangnya teknologi, kini dokumen tidak hanya diproduksi dalam bentuk cetak saja tetapi diproduksi juga dalam bentuk digital, khususnya dokumen gambar. Keuntungan dokumen digital yaitu lebih mudah dan efisien dalam penggunaannya tetapi dokumen digital pun mudah untuk dipalsukan. Untuk mengatasi hal tersebut, dibutuhkanlah suatu teknik keamanan dokumen digital yaitu dokumen diberi tanda tangan digital. Penelitian ini bertujuan untuk menjelaskan proses implementasi *Digital Signature Algorithm* dengan menggunakan fungsi hash, yaitu *Secure Hash Algorithm-256* pada media gambar serta merancang program tanda tangan digital.

Hasil dari penelitian ini menunjukkan bahwa *Digital Signature Algorithm* (DSA) menggunakan fungsi hash *Secure Hash Algorithm-256* tidak hanya dapat diimplementasikan pada pesan teks, namun dapat diimplementasikan pada media gambar dengan metode konversi gambar menjadi gambar ASCII. DSA juga dapat dibuat program menggunakan Bahasa pemrograman Python guna mempermudah dalam pembangkitan dan autentikasi tanda tangan.

**Kata Kunci :** Kriptografi, fungsi hash, kunci asimetris, *Digital Signature Algorithm*, *Secure Hash Algorithm-256*

## ABSTRACT

With the development of technology, documents not only produced in printed form but also produced in digital form, especially image documents. The advantage of digital documents is that they are easier and more efficient to use but digital documents are also easy to fake. To overcome this, a digital document security technique is needed, that is the document is digitally signed. This study aims to explain the process of implementing *Digital Signature Algorithm* by using the *Secure Hash Algorithm-256* as hash function on image file and designing digital signature programs.

The results of this study indicate that the *Digital Signature Algorithm* (DSA) using the *Secure Hash Algorithm-256* hash function can't only be implemented in text messages, but can be implemented in image file by the method of image conversion to ASCII images. DSA can also be programmed using the Python programming language to facilitate the generation and authentication of signatures.

**Keywords:** Cryptography, hash function, asymmetric key, *Digital Signature Algorithm*, *Secure Hash Algorithm-256*

## DAFTAR ISI

LEMBAR PENGESAHAN	
PERNYATAAN	
KATA PENGANTAR .....	i
UCAPAN TERIMA KASIH.....	ii
ABSTRAK .....	iv
ABSTRACT.....	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR .....	ix
DAFTAR TABEL.....	x
DAFTAR LAMPIRAN.....	xi
BAB I PENDAHULUAN .....	1
1.1 Latar belakang .....	1
1.2 Rumusan masalah.....	3
1.3 Tujuan Penelitian.....	4
1.4 Batasan Masalah.....	4
1.5 Manfaat Penelitian.....	4
1.6 Sistematika Penulisan.....	4
BAB II LANDASAN TEORI .....	6
2.1 Aritmetika Modulo .....	6
2.2 Kongruen .....	6
2.3 <i>Bit-wise</i> .....	8
2.3.1 <i>NOT</i> .....	8
2.3.2 <i>AND</i> .....	8

2.3.3	<i>OR</i> .....	8
2.3.4	<i>XOR</i> .....	9
2.4	<i>Bit-shifts</i> .....	9
2.4.1	<i>Arithmetic shift</i> .....	9
2.4.2	<i>Circular-shift</i> atau <i>Rotate</i> .....	10
2.5	Fungsi Hash (Maryanto, 2008).....	10
2.6	Secure Hash Algorithm (SHA).....	12
2.7	Secure hash Algorithm-256 (SHA-256).....	12
2.8	Digital Signature Algorithm (DSA) .....	15
2.9	Sistem ASCII.....	18
2.10	Bahasa Pemrograman Python .....	19
BAB III METODOLOGI PENELITIAN.....		20
3.1	Identifikasi Masalah .....	20
3.2	Model Dasar .....	20
3.3	Pengembangan Model .....	20
3.3.1	Pembangkitan Kunci .....	21
3.3.2	Hashing Pada Media Gambar.....	22
3.3.3	Pembentukan dan Autentikasi Tanda Tangan.....	26
3.4	Pembuatan Program Komputer .....	27
3.4.1	Input dan Output .....	27
3.4.2	Rancangan Antarmuka Program .....	28
3.4.3	<i>Pseudocode</i> DSA .....	29
3.5	Validasi.....	30
BAB IV HASIL DAN PEMBAHASAN .....		31

4.1	Hasil Program.....	31
4.1.1	Antarmuka Program.....	31
4.1.2	Petunjuk Penggunaan Program .....	34
4.2	Validasi Program.....	36
4.2.1	Pembangkit bilangan prima.....	37
4.2.2	Pembangkitan Kunci .....	38
4.2.3	Pembangkitan Tanda Tangan Digital.....	39
4.3.4	Autentikasi Tanda Tangan Digital .....	43
BAB V KESIMPULAN DAN SARAN.....		48
5.1	Kesimpulan.....	48
5.2	Saran.....	48
DAFTAR PUSTAKA .....		50
LAMPIRAN.....		52



## DAFTAR GAMBAR

Gambar 2.1 Terjadi tumbukan pada pesan A dan B .....	11
Gambar 2.2 Karakteristik beberapa macam fungsi hash.....	11
Gambar 3.1 <i>Flowchart</i> pengembangan <i>Digital Signature Algorithm</i> .....	21
Gambar 3.2 proses <i>hashing</i> pesan gambar.....	22
Gambar 3.3 Warna <i>grayscale</i> .....	24
Gambar 3.4 Membuat interval warna.....	24
Gambar 3.5 Melakukan pemetaan untuk setiap interval warna. ....	25
Gambar 3.6 Rancangan tampilan utama program DSA.....	28
Gambar 3.7 Rancangan menu pembangkit kunci. ....	28
Gambar 3.8 Rancangan menu pembangkit tanda tangan digital.....	29
Gambar 3.9 Rancangan menu autentikasi tanda tangan digital. ....	29
Gambar 4.1 Antarmuka program DS Generator .....	32
Gambar 4.2 Menu Pembangkit Kunci Digital pada DS Generator .....	32
Gambar 4.3 Menu Pembangkit Tanda Tangan Digital pada DS Generator .....	33
Gambar 4.4 Menu Autentikasi Tanda Tangan Digital pada DS Generator .....	33
Gambar 4.5 Input program Prime Generator. ....	34
Gambar 4.6 Output proses pencarian di program Prime Generator.....	35
Gambar 4.7 Logo UPI.....	39
Gambar 4.8 <i>Grayscale</i> Logo UPI.....	39
Gambar 4.9 <i>ASCII art</i> Logo UPI.....	40
Gambar 4.10 <i>ASCII art</i> Logo UPI ketika di <i>zoom</i> .....	40
Gambar 4.11 Gambar B .....	46

**DAFTAR TABEL**

Tabel 2.1 Contoh fungsi hash.....	12
Tabel 3.1 Inisialisasi karakter. ....	23

**DAFTAR LAMPIRAN**

Lampiran 1: <i>ASCII table printable characters</i> .....	52
Lampiran 2 : Coding program <i>Digital Signature</i> .....	53

## DAFTAR PUSTAKA

- Azdy, R. A. (2016). Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi (JNTETI)*, 5(3), 184–191. <https://doi.org/10.22146/jnteti.v5i3.255>
- Durbin, J. R. (2009). *Modern Algebra: An Introduction, 6th ed.* (L. R. S. Corliss (ed.); 6th ed.). Laurie Rosatone.
- IONOS. (2019, August 5). *ASCII-Codes | All symbols & characters on the ASCII table - IONOS*. <https://www.ionos.com/digitalguide/server/know-how/ascii-codes-overview-of-all-characters-on-the-ascii-table/>
- Jacob, F. W. (2012, July 17). *Faster Bit Rotation*. <https://www.codeproject.com/Tips/423258/Faster-Bit-Rotation>
- Killian, J. (2012, April 18). *Understanding Bitwise Operators*. <https://code.tutsplus.com/articles/understanding-bitwise-operators--active-11301>
- Lundh, F., & Clark, A. (2020). *Overview — Pillow (PIL Fork) 7.2.0 documentation*. <https://pillow.readthedocs.io/en/stable/handbook/overview.html>
- Lutz, M. (2001). *Programming Python* (L. Lewin, F. Willison, & E. Quill (eds.); 2nd ed.). O'Reilly & associates, inc., 101 Morris street, Sebastopol, CA 95472.
- Maryanto, B. (2008). Penggunaan Fungsi Hash Satu-Arah untuk Enkripsi Data. *Media Informatika*, 7(3), 1–10.
- MateriDosen. (2015, October 17). *Pengertian dan Fungsi Kode ASCII (Lengkap) - Materi Dosen*. <http://www.materidosen.com/2016/10/pengertian-dan-fungsi-kode-ascii-lengkap.html>
- Mayasari, N., & Arpan. (2019). *MEMBANGKITKAN DIGITAL SIGNATURE DENGAN ALGORITMA MD5 DAN ALGORITMA RSA UNTUK*. 6, 8–13.
- Munir, R. (2005). Penggunaan Tanda-Tangan Digital Untuk Menjaga Integritas Berkas Perangkat Lunak. *Seminar Nasional Aplikasi Teknologi Informasi 2005, 2005(Snati)*, 6–9.
- Munir, R. (2010). *MATEMATIKA DISKRIT* (3rd ed.). Informatika Bandung.

- Munir, R. (2017). *Protokol Kriptografi Bahan Kuliah Protokol*.
- Munir, R. (2018). *Digital Signature Standard (DSS) Bahan Kuliah IF4020 Kriptografi*.
- Precilia, D. P., & Izzuddin, A. (2016). Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5). *Energy*, 5(1), 14–19.
- Prihardhanto, M. D. (2010). *Studi Perbandingan Beberapa Fungsi Hash dalam Melakukan Checksum Berkas*.
- RosettaCode. (2020, April 30). *SHA-256 - Rosetta Code*. <https://rosettacode.org/wiki/SHA-256>
- Sakti, D. V. S. Y., Agani, N., & Hardjianto, M. (2016). Pengamanan Sistem Menggunakan One Time Password Dengan Pembangkit Password Hash SHA-256 dan Pseudo Random Number Generator (PRNG) Linear Congruential Generator (LCG) di Perangkat Berbasis Android. *Conference: Budi Luhur Information Technology, At Budi Luhur University, Volume: 13 No. 1, 13(1)*, 1–3.
- Sembiring, J. (2013). Analisis Algoritma Sha-512 Dan Watermarking Dengan Metode Least Significant Bit Pada Data Citra. *Seminar Nasional Sistem Informasi Indonesia*, 2–4.
- Stevens Marc, Bursztein Elie, Karpman Pierre, Albertini Ange, Markov Yarik, Bianco Alex Petit, & Baisse Clement. (2017, January 23). *Google Online Security Blog: Announcing the first SHA1 collision*. <https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>
- Widarsha, C. S. (2019, January 11). *Bupati Bondowoso Polisikan Warga yang Palsukan Tanda Tangannya*. <https://news.detik.com/berita-jawa-timur/d-4604018/bupati-bondowoso-polisikan-warga-yang-palsukan-tanda-tangannya>
- Xie, T., Liu, F., & Feng, D. (2006). Fast collision attack on MD5. *IACR EPrint Archive Report*, 104, 17. <https://doi.org/10.1.1.301.4421>