Perbandingan Kinerja Algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) Menggunakan Fungsi *Hash Secure Hash Algorithm* (SHA-1) dan Keccak pada Tanda Tangan Digital

Tugas Akhir

Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Oleh :

Nur Annisa Fitriani
(201610370311015)

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2021**

LEMBAR PERSETUJUAN

Perbandingan Kinerja Algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) Menggunakan Fungsi *Hash Secure Hash Algorithm* (SHA-1) dan Keccak pada Tanda Tangan Digital

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana Strata 1
Teknik Informatika Universitas Muhammadiyah Malang

Nur Annisa Fitriani
201610370311015

Menyetujui,
Malang, 4 /01/ 2021

Dosen I

Dosen II

Aminudin, S.Kom, M.Cs
NIDN. 070168603

Sofyan Arifianto, S.Si, M.Kom
NIDN. 0721058309

LEMBAR PENGESAHAN

Perbandingan Kinerja Algoritma *Elliptic Curve Digital Signature Algorithm*
(ECDSA) Menggunakan Fungsi *Hash Secure Hash Algorithm* (SHA-1) dan
Keccak pada Tanda Tangan Digital

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana Strata 1
Teknik Informatika Universitas Muhammadiyah Malang

Nur Annisa Fitriani
201610370311015

Menyetujui,
Malang, 2 / 2 / 2021

Penguji I

Svaifuddin, S.Kom, M.Kom
NIDN. 076118701

Penguji II

Denar Regata Akbi, S.Kom, M.Kom
NIDN. 0701058601

Mengetahui
Ketua Program Studi Teknik Informatika

Gita Indah Marthasari, ST, M.Kom
NIDN. 0720038101

LEMBAR PERNYATAAN

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Nur Annisa Fitriani
Tempat,Tgl Lahir : Buntok, 04 September 1998
NIM : 201610370311015
Fakultas/Jurusan : Teknik Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul “Perbandingan Kinerja Algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) menggunakan Fungsi Hash *Secure Hash Algorithm* (SHA-1) dan Keccak pada Tanda Tangan Digital” beserta isinya adalah karya saya sendiri dan bukan merupakan karya tulisan orang lain, baik iiiay aini atau seluruhnya, kecuali bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko atau sanksi yang berlaku.

Menyetujui,
Malang, 3 /01/ 2021

Mengetahui,
Dosen Pembimbing,

Aminudin, S.Kom, M.Cs.
NIP. 108.1703.0594

Malang,
Yang membuat pernyataan

Nur Annisa Fitriani
NIM. 201610370311015

ABSTRAK

Sebuah data atau dokumen yang dikirimkan melalui internet sangat rentan terhadap serangan atau modifikasi serta sangat sulit untuk membuktikan keaslian data atau dokumen, maka dengan perkembangan sistem keamanan terbentuklah sebuah mekanisme kriptografi yang digunakan untuk memverifikasi keaslian dan kebenaran dari sebuah data yang disebut dengan tanda tangan digital. Tanda tangan digital seringkali dipadukan dengan fungsi hash untuk membuat tanda tangan pada suatu data. Algoritma tanda tangan yang sering digunakan adalah *Diffle-Helman Digital Signature Algorithm* dan lebih dikenal sebagai *Digital Signature Algorithm (DSA)*. Algoritma *Digital Signature Algorithm (DSA)* dikembangkan menjadi algoritma *Elliptic Curve Digital Signature Algorithm (ECDSA)* yang menggunakan *elliptic curve*. Penelitian ini Melakukan perbandingan kinerja algoritma tanda tangan digital *Elliptic Curve Digital Signature Algorithm (ECDSA)* menggunakan fungsi hash yang berbeda dan menganalisis performa waktu proses dari awal hingga akhir antara algoritma *Elliptic Curve Digital Signature Algorithm (ECDSA)* menggunakan fungsi hash SHA-1 dan algoritma *Elliptic Curve Digital Signature Algorithm (ECDSA)* menggunakan fungsi hash Keccak. Parameter pengujian yang dilakukan membandingkan algoritma *Elliptic Curve Digital Signature Algorithm (ECDSA)* fungsi hash SHA-1 dan Keccak pada saat proses pembangkitan kunci (*key generation*), tahap penandatanganan (*signature generation*), dan tahap verifikasi tanda tangan digital (*verifying*).

Kata Kunci – Tanda tangan digital, Algoritma ECDSA, SHA-1, Keccak (SHA-3)

ABSTRACT

Data or document sent over the internet is very vulnerable to attack or modification and it is very difficult to prove the authenticity of data or documents, so with the development of a security system a cryptography is formed which is used to verify the authenticity and truth of a data called a digital signature. Digital signatures are combined with hash functions to create signatures on data. The signature algorithm that is often used is the Diffie-Hellman Digital Signature Algorithm and is better known as the Digital Signature Algorithm (DSA). The Digital Signature Algorithm (DSA) algorithm was developed into an Elliptic Curve Digital Signature Algorithm (ECDSA) algorithm that uses an elliptic curve. This study compares the great performance of the digital signature Elliptic Curve Digital Signature Algorithm (ECDSA) using different hash functions and the performance of analyzing processing time from start to finish between ECDSA algorithm using SHA-1 hash function and ECDSA algorithm using Keccak hash function. Parameter testing is carried out comparing the ECDSA algorithm of SHA-1 and Keccak hash functions during the key generation process (key generation), the signing stage (signature generation), and the digital signature leveraging stage (verification).

Keywords – Digital Signature, Elliptic Curve Digital Signature Algorithm (ECDSA), SHA-1, Keccak (SHA-3)

LEMBAR PERSEMBAHAN

Puji dan syukur kehadiran Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, dan tak lupa shalawat serta salam kepada junjungan Nabi Muhammad SAW, sehingga dengan ridha-Nya skripsi yang berjudul “Perbandingan Kinerja Algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) menggunakan Fungsi Hash *Secure Hash Algorithm* (SHA-1) dan Keccak pada Tanda Tangan Digital” dapat terselesaikan.

Penyelesaian tugas akhir ini tidak lepas dari dukungan dan bantuan dari berbagai pihak, baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis dengan segala kerendahan hati menyampaikan ucapan terimakasih yang sebesar-besarnya kepada :

1. Allah SWT yang selalu memberikan kemudahan dan kesabaran dalam mengerjakan tugas akhir ini.
2. Kedua orang tua tercinta, Bapak Noor Hasani, Ibu Juraida, kedua adik saya Nabella dan Ilmi yang selalu memberikan do’a dan dukungan kepada penulis secara moril maupun materil sehingga Tugas Akhir ini dapat selesai.
3. Bapak Aminudin, S.Kom, M.Cs. selaku dosen pembimbing I yang telah memberikan bimbingan, arahan, serta saran kepada penulis dalam penelitian Tugas Akhir.
4. Sofyan Arifianto S.Si, M.Kom selaku dosen pembimbing II yang telah memberikan bimbingan, arahan, serta saran kepada penulis dalam penelitian Tugas Akhir.
5. Ibu Gita Indah Marthasari, S.T, M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Muhammadiyah Malang.
6. Seluruh Bapak dan Ibu Dosen Pengajar yang telah memberikan ilmunya dan Staff TU jurusan Informatika.
7. Teman seperjuangan saya Nabilah Arwa yang selalu memberikan semangat dan motivasi dalam segala bentuk mulai dari awal kuliah hingga pengerjaan tugas akhir ini selesai.
8. Teman-teman saya Imsa, Vincia, Riri, Salsa dan Yudanty yang selalu memberikan semangat, dukungan, motivasi, dan saran kepada saya.
9. Sahabat saya Nor Harisha yang selalu memberikan dukungan, motivasi, semangat dan mendengarkan semua keluhan saya.
10. Teman-teman kelas Informatika A 2016 yang selalu memberi dukungan dan motivasi kepada saya selama ini dan teman-teman saya yang tidak dapat saya sebutkan satu per satu, terimakasih atas segala dukungan dan motivasi.

KATA PENGANTAR

Puji syukur kehadiran Allah Subhanahu Wa Ta'ala atas limpahan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul “Perbandingan Kinerja Algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) menggunakan Fungsi Hash *Secure Hash Algorithm* (SHA-1) dan Keccak pada Tanda Tangan Digital”. Tulisan ini disajikan pokok-pokok bahasan yang meliputi latar belakang, metode penelitian, dan hasil dan pembahasan yang telah didapat dari penelitian ini telah disimpulkan berdasarkan hasil yang telah didapat oleh peneliti. Peneliti menyadari sepenuhnya bahwa dalam penulisan tugas akhir ini masih banyak kekurangan dan keterbatasan. Oleh karena itu, peneliti sangat mengharapkan saran yang membangun agar tulisan ini bermanfaat untuk perkembangan ilmu pengetahuan kedepan.

Malang, 03 January 2021

Penulis

Nur Annisa Fitriani

DAFTAR ISI

LEMBAR PERSETUJUAN	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN	iii
ABSTRAK	iii
ABSTRACT	v
LEMBAR PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xii
DAFTAR LAMPIRAN	xiii
BAB 1	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian	3
1.4 Batasan Masalah	3
1.5 Penyusunan Laporan	4
1.6 Sistematika Penelitian	4
BAB 2	5
2.1. Tanda Tangan Digital (<i>Digital Signature</i>)	5
2.2. <i>Elliptic Curve Digital Signature Algorithm</i> (ECDSA)	7
2.3. Fungsi Hash	8
2.3.1. SHA-1	8
2.3.2. Keccak (SHA-3)	9
2.4 Import Library	11
2.5 Skenario Pengujian	12

BAB 3	13
3.1. Analisa Masalah	13
3.2. Rancangan Implementasi	13
3.2.1. <i>Elliptic Curve Digital Signature Algorithm</i> (ECDSA)	13
3.2.2. Fungsi Hash	14
3.2.2.1 SHA-1	14
3.2.2.2 Keccak (SHA-3)	15
3.3. Skenario Pengujian	16
3.3.1 Pengujian algoritma ECDSA menggunakan fungsi hash SHA-1	17
3.3.2 Pengujian algoritma ECDSA menggunakan fungsi hash Keccak (SHA-3)	18
BAB 4	20
4.1 Implementaasi	20
4.1.1 Implementasi Perangkat Keras	20
4.1.2 Implementasi Perangkat Lunak	20
4.1.3 Import Library	20
4.1.4 Implementasi Algoritma ECDSA menggunakan 2 Fungsi Hash	21
4.1.4.1 Implementasi Algoritma ECDSA menggunakan Fungsi Hash SHA-1	21
4.1.4.2 Implementasi Algortima ECDSA menggunakan Fungsi Hash Keccak (SHA-3)	21
4.2 Pengujian	22
4.2.1 Pengujian Algoritma ECDSA menggunakan Fungsi Hash SHA-1	22
4.2.2 Pengujian Algoritma ECDSA menggunakan Fungsi Hash Keccak	27
4.3 Hasil Analisa Perbandingan ECDSA menggunakan Fungsi Hash SHA-1 dan ECDSA menggunakan Fungsi Hash Keccak	33
BAB 5	35
5.1 Kesimpulann	35
5.2 Saran	35
DAFTAR PUSTAKA	36

DAFTAR GAMBAR

Gambar 2.1 Proses Tanda Tangan Digital.....	6
Gambar 2.2 Ilustrasi konstruksi spons	10
Gambar 2.3 <i>library</i> ecdsa yang digunakan oleh starkbank	11
Gambar 3.1 <i>Pseudocode</i> Algoritma ECDSA	14
Gambar 3.2 <i>Pseudocode</i> SHA-1.....	14
Gambar 3.3 <i>Pseudocode</i> θ (<i>theta</i>)	15
Gambar 3.4 <i>Pseudocode</i> ρ (<i>rho</i>).....	15
Gambar 3.5 <i>Pseudocode</i> π (<i>pi</i>).....	15
Gambar 3.6 <i>Pseudocode</i> χ (<i>chi</i>)	16
Gambar 3.7 <i>Pseudocode</i> ι (<i>iota</i>).....	16
Gambar 3.8 <i>Pseudocode</i> ι (<i>iota</i>).....	16
Gambar 4.1 hasil inputan text 1 dihash menggunakan fungsi hash SHA-1	22
Gambar 4.2 hasil inputan text 2 dihash menggunakan fungsi hash SHA-1.....	23
Gambar 4.3 hasil inputan text 3 dihash menggunakan fungsi hash SHA-1	24
Gambar 4.4 hasil inputan text 4 dihash menggunakan fungsi hash SHA-1	25
Gambar 4.5 hasil inputan text 5 dihash menggunakan fungsi hash SHA-1	26
Gambar 4.6 hasil inputan text 1 dihash menggunakan fungsi hash Keccak	28
Gambar 4.7 hasil inputan text 2 dihash menggunakan fungsi hash Keccak	29
Gambar 4.8 hasil inputan text 3 dihash menggunakan fungsi hash Keccak	30
Gambar 4.9 hasil inputan text 4 dihash menggunakan fungsi hash Keccak	31
Gambar 4.10 hasil inputan text 4 dihash menggunakan fungsi hash Keccak	32
Gambar 4.11 Grafik Perbandingan Hasil Waktu Pembangkitan Kunci, Tanda Tangan, dan Verifikasi Algoritma ECDSA menggunakan fungsi hash SHA-1 dan Keccak pada Text 1, Text 2, Text 3, Text 4, dan Text 5.....	33

DAFTAR TABEL

Tabel 4.1 Hasil scenario pengujian algoritma ECDSA menggunakan fungsi hash SHA-1 inputan text 1	23
Tabel 4.2 Hasil scenario pengujian algoritma ECDSA menggunakan fungsi hash SHA-1 inputan text 2	24
Tabel 4.3 Hasil scenario pengujian algoritma ECDSA menggunakan fungsi hash SHA-1 inputan text 3	25
Tabel 4.4 Hasil scenario pengujian algoritma ECDSA menggunakan fungsi hash SHA-1 inputan text 4	26
Tabel 4.5 Hasil scenario pengujian algoritma ECDSA menggunakan fungsi hash SHA-1 inputn text 4	27
Tabel 4.6 Hasil scenario pengujian algoritma ECDSA menggunakan fungsi hash Keccak inputan text 1	28
Tabel 4.7 Hasil scenario pengujian algoritma ECDSA menggunakan fungsi hash Keccak inputan text 2	29
Tabel 4.8 Hasil scenario pengujian algoritma ECDSA menggunakan fungsi hash Keccak inputan text 3	30
Tabel 4.9 Hasil scenario pengujian algoritma ECDSA menggunakan fungsi hash Keccak inputan text 4	31
Tabel 4.10 Hasil scenario pengujian algoritma ECDSA menggunakan fungsi hash Keccak inputan text 5	32

DAFTAR LAMPIRAN

Gambar 1. Tampilan masukkan inputan text.....	38
Gambar 2. Tampilan isi pesan yang telah dihash	38
Gambar 3. Tampilan <i>publik key</i> , waktu proses generate <i>publik key</i> dan proses <i>signature</i> SHA-1	39
Gambar 4. Tampilan waktu proses <i>generate signature</i> , verifikasi, dan waktu proses verifikasi SHA-1	39
Gambar 5. Tampilan <i>public key</i> , waktu proses generate <i>public key</i> dan proses <i>signature</i> SHA-3 (Keccak)	39
Gambar 6 . Tampilan waktu proses <i>generate signature</i> , verifikasi, dan waktu proses verifikasi SHA-3 (Keccak)	40
Gambar 7. Source Code import library	40
Gambar 8. Source Code EC.php	46
Gambar 9. Source Code File.php	46
Gambar 10. Source Code Ecdsa.php	47
Gambar 11. Source Code PrivateKey.php.....	49
Gambar 12. Source Code PublikKey.php	50
Gambar 13. Source Code Signature.php	51
Gambar 14. Source Code Panjang Kurva Elliptic Curve	51
Gambar 15. Source Code Pembangkitan Kunci Algoritma ECDSA menggunakan Fungsi Hash SHA-1	52
Gambar 16. Source Code Pemberian Tanda Tangan Algoritma ECDSA menggunakan Fungsi Hash SHA-1.....	52
Gambar 17. Source Code Verifikasi Tanda Tangan Digital Algoritma ECDSA menggunakan Fungsi Hash SHA-1.....	53
Gambar 18. Source Code Pembangkitan Kunci Algoritma ECDSA menggunakan Fungsi Hash Keccak	54

Gambar 19. <i>Source Code</i> Pemberian Tanda Tangan Algoritma ECDSA menggunakan Fungsi Hash Keccak	55
Gambar 20. <i>Source Code</i> Verifikasi Tanda Tangan Digital Algoritma ECDSA menggunakan Fungsi Hash Keccak	56

DAFTAR PUSTAKA

- [1] V. Kusuma, J. Matematika, dan F. Matematika, “Elliptic Curve dan Implementasinya pada Algoritma Tanda Tangan Digital,” *J. Sains dan Seni ITS*, vol. 3, no. 2, hal. 3–6, Sep 2014.
- [2] D. W. R, “Perbandingan Algoritma Berbasis Elliptic Curve Cryptography Dengan RSA dan DSA Pada Tanda Tangan Digital,” *Inform. STEI ITB*, vol. 2, no. 1, hal. 1–7, 2007.
- [3] R. A. Azdy, “Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA,” *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 5, no. 3, hal. 184–191, 2016, doi: 10.22146/jnteti.v5i3.255.
- [4] H. Azhar, “Perbandingan Algoritma Fungsi Hash MD5 dengan SHA-1,” 2013.
- [5] M. Y. Soleh dan S. Teknik, “Studi dan Implementasi Algoritma Keccak,” 2011.
- [6] V. Kusuma, J. Matematika, dan F. Matematika, “Elliptic Curve dan Implementasinya pada Algoritma Tanda Tangan Digital,” vol. 3, no. 2, hal. 3–6, 2014.
- [7] D. A. Rahman, “Pemanfaatan Tanda Tangan Digital Menggunakan ECDSA dan Keccak pada Teks Editor,” 2018.
- [8] K. Yauris, “Penggunaan Fungsi Hash dan Tanda Tangan Digital dalam Transmisi Data,” *Makal. ke-2 IF4020 Kriptografi, Semester II Tahun 2015/2016*, 2016.
- [9] R. Munir, “Kriptografi.” Informatika Bandung, Bandung, hal. 880, 2019.
- [10] T. N. Ovari, “Implementasi Elliptic Curve Digital Signature Algorithm (ECDSA) untuk Mengatasi Black Hole dan Worm Hole Attack pada Komunikasi V2V di Lingkungan VANETs,” hal. 93, 2017.
- [11] V. K. Pesan *et al.*, “IMPLEMENTASI ALGORITMA ECDSA UNTUK PENGAMANAN E-MAIL 2 . Tinjauan Pustaka 2 . 3 ECDSA (Elliptical Curve Digital Signature).”
- [12] W. A. Triyanto, “CLASS LIBRARY UNTUK PEMBUATAN APLIKASI CRUD

Wiwit Agus Triyanto Program Studi Sistem Informasi, Fakultas Teknik, Universitas Muria Kudus Gondangmanis, PO Box 53, Bae, Kudus 59352,” *Pros. SNATIF Ke-1*, hal. 349–356, 2014.

- [13] D. Toradmalle, R. Singh, H. Shastri, N. Naik, dan V. Panchidi, “Prominence of ECDSA over RSA digital signature algorithm,” *Proc. Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud), I-SMAC 2018*, hal. 253–257, 2019, doi: 10.1109/I-SMAC.2018.8653689.

UNIVERSITAS MUHAMMADIYAH MALANG
FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK INFORMATIKA
Jl. Raya Tlogomas 246 Malang 65144 Telp. 0341 - 460118 Ext. 247, Fax. 0341 - 460782

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : Nur Annisa Fitriani
NIM : 201610370311015
Judul TA : Perbandingan Kinerja Algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) menggunakan Fungsi Hash *Secure Hash Algorithm* (SHA-1) dan Keacak pada Tanda Tangan Digital

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	0 %
2.	Bab 2 – Daftar Pustaka	25 %	10 %
3.	Bab 3 – Analisis dan Perancangan	25 %	10 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	9 %
5.	Bab 5 – Kesimpulan dan Saran	5 %	3 %
6.	Makalah Tugas Akhir	20%	11 %

*) Hasil cek plagiarisme diisi oleh salah satu pembimbing

*) Maksimal 5 kali

Mengetahui,
Dosen Pembimbing

Amrudin, S.Kom, M.Cs)