

**IMPLEMENTASI *ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM*
DAN *SECURE HASH ALGORITHM 256* PADA LOGIN AKUN
DENGAN SISTEM *TWO-FACTOR AUTHENTICATION***

SKRIPSI

Diajukan untuk memenuhi sebagian syarat memperoleh gelar Sarjana Matematika



Oleh:

Hokianto Suseno

NIM 2101111

**PROGRAM STUDI MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
2025**

LEMBAR HAK CIPTA

**IMPLEMENTASI *ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM*
DAN *SECURE HASH ALGORITHM 256* PADA LOGIN AKUN
DENGAN SISTEM *TWO-FACTOR AUTHENTICATION***

Oleh:

Hokianto Suseno

2101111

Diajukan untuk memenuhi sebagian syarat memperoleh gelar Sarjana Matematika
pada Program Studi Matematika Fakultas Pendidikan Matematika dan Ilmu
Pengetahuan Alam

© Hokianto Suseno

Universitas Pendidikan Indonesia

April 2025

Hak Cipta dilindungi undang-undang

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian dengan dicetak
ulang, difotokopi, atau cara lainnya tanpa izin penulis.

LEMBAR PENGESAHAN

HOKIANTO SUSENO

IMPLEMENTASI *ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM*
DAN *SECURE HASH ALGORITHM 256* PADA LOGIN AKUN
DENGAN SISTEM *TWO-FACTOR AUTHENTICATION*

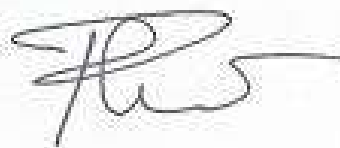
Disetujui dan disahkan,

Pembimbing I



Prof. Siti Fatimah, M.Si., Ph.D.
NIP. 19680823199432002

Pembimbing II



Dra. Hj. Rini Marwati, M.S.
NIP.196606251990012001

Mengetahui,

Ketua Program Studi Matematika



Dr. Kartika Yulianti, M.Si.
NIP. 198207282005012001

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul “Implementasi *Elliptic Curve Digital Signature Algorithm* dan *Secure Hash 256* pada Login Akun dengan Sistem *Two-Factor Authentication*” ini beserta seluruh isi di dalamnya adalah benar-benar karya saya sendiri. Saya tidak melakukan plagiarisme atau mengutip dengan cara yang melanggar norma-norma etika keilmuan yang berlaku. Dengan pernyataan ini, saya bersedia menerima konsekuensi atau sanksi apa pun jika di kemudian hari terbukti terdapat pelanggaran etika akademik atau ada klaim dari pihak lain atas keaslian karya ini.

Bandung, April 2025

Yang Membuat Pernyataan

A yellow rectangular official stamp from Universitas Padjadjaran (UNPAD) is visible. It features the university's logo and the text "UNIVERSITAS PADJADJARAN" and "FAKULTAS TEKNIK". A handwritten signature in black ink is written over the stamp. Below the stamp, the name "Hokianto Suseno" is printed in bold black text.

NIM. 2101111

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi yang berjudul “Implementasi *Elliptic Curve Digital Signature Algorithm* dan *Secure Hash Algorithm 256* pada Login Akun dengan Sistem *Two-Factor Authentication*” sebagai salah satu syarat memperoleh gelar Sarjana Matematika di Universitas Pendidikan Indonesia (UPI). Selama proses penulisannya, penulis menghadapi banyak tantangan dan hambatan, namun berkat bantuan dan dorongan dari berbagai pihak, skripsi ini dapat terselesaikan dengan baik.

Penulis menyadari bahwa masih terdapat kekurangan dalam penyusunan skripsi ini dikarenakan keterbatasan pengetahuan dan pengalaman yang dimiliki penulis. Oleh karena itu, kritik dan saran yang membangun sangat diperlukan guna menyempurnakan dan mengembangkan skripsi ini. Penulis berharap skripsi ini dapat bermanfaat bagi para pembaca, khususnya yang sedang mendalami sistem keamanan akun dan kriptografi.

Bandung, April 2025

Penulis

UCAPAN TERIMA KASIH

Dalam penulisan skripsi ini, penulis mendapatkan banyak bimbingan, dukungan dan doa dari berbagai pihak. Untuk itu, penulis ucapkan terima kasih kepada:

1. Ibu Prof. Siti Fatimah, Ph.D. selaku dosen pembimbing I yang telah meluangkan waktunya untuk membimbing dan memberi arahan kepada penulis selama penulisan skripsi.
2. Ibu Dra. Hj. Rini Marwati, M.S. selaku dosen pembimbing II yang telah meluangkan waktunya untuk membimbing dan memberi arahan kepada penulis selama penulisan skripsi.
3. Orang tua yang selalu mendoakan dan memberikan dukungan, serta kakak penulis yang juga telah memberikan doa dan dukungan.
4. Seluruh dosen dan civitas akademika di lingkungan program studi Matematika, Universitas Pendidikan Indonesia.
5. Sahabat-sahabat penulis yang telah memberikan dukungan khususnya Arya Shidika Listanto dan Bagas Ghulam Maulana yang menyediakan tempat berupa kos-kosan untuk menyelesaikan skripsi, serta “Tas Merah” yang selalu memberi bantuan, dukungan, dan kebersamaan.
6. Rekan-rekan mahasiswa Matematika UPI yang telah memberikan doa, dukungan, dan motivasi kepada penulis.
7. Pihak lainnya yang tidak dapat disebutkan satu per satu yang juga telah memberikan dukungan.

Semoga segala bentuk dukungan, doa, dan keabikan mendapatkan balasan dari Tuhan Yang Maha Esa.

ABSTRAK

Autentikasi dua faktor (2FA) merupakan metode keamanan yang semakin banyak digunakan untuk meningkatkan keamanan login akun. Penelitian ini membahas implementasi algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) dan *Secure Hash Algorithm 256* (SHA 256) dalam sistem 2FA. ECDSA digunakan untuk menghasilkan tanda tangan digital sebagai bukti keaslian pengguna, sedangkan SHA 256 diterapkan dalam proses *hashing* untuk melindungi informasi sensitif, seperti *username*, *password*, dan kunci privat. Proses autentikasi terdiri dari dua tahap utama, yaitu verifikasi *username* dan *password* pengguna, serta validasi tanda tangan digital. Jika *username* dan *password* benar, *server* mengirimkan pesan acak kepada *client* untuk ditandatangani menggunakan kunci privat ECDSA, lalu hasil tanda tangan dikirim kembali ke *server* untuk diverifikasi menggunakan kunci publik. Implementasi dilakukan menggunakan bahasa pemrograman Python dengan penyimpanan berbasis *file txt*. Hasil pengujian menunjukkan bahwa metode ini mampu meningkatkan keamanan autentikasi dengan mencegah akses tanpa izin, meskipun masih memerlukan optimasi lebih lanjut dalam aspek efisiensi dan pengelolaan kunci privat. Selanjutnya, sistem ini dapat dikembangkan lebih lanjut dengan menggunakan basis data untuk penyimpanan yang lebih aman, serta diimplementasikan dalam aplikasi berbasis *web* atau *mobile* agar lebih mudah diadopsi secara luas.

Kata Kunci: Autentikasi Dua Faktor, Elliptic Curve Digital Signature Algorithm, Keamanan Akun, Secure Hash Algorithm 256, Tanda Tangan Digital

ABTRACT

Two-factor authentication (2FA) is a security method that is increasingly being used to improve account login security. This research discusses the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) and Secure Hash Algorithm 256 (SHA 256) algorithms in a 2FA system. ECDSA is used to generate digital signatures as proof of user authenticity, while SHA 256 is applied in the hashing process to protect sensitive information, such as usernames, passwords and private keys. The authentication process consists of two main stages, such as verifying the user's username and password, and validating the digital signature. If the username and password are correct, the server sends a random message to the client to be signed using the ECDSA private key, then the signature results are sent back to the server to be verified using the public key. Implementation is carried out using the Python programming language with txt file-based storage. Test results show that this method is able to increase authentication security by preventing unauthorized access, although it still requires further optimization in terms of efficiency and private key management. Furthermore, this system can be further developed by using a database for safer storage, as well as implemented in a web-based or mobile application to make it easier to adopt widely.

Keyword: *Account Security, Digital Signature, Elliptic Curve Digital Signature Algorithm, Secure Hash Algorithm 256, Two-Factor Authentication*

DAFTAR ISI

LEMBAR HAK CIPTA i

LEMBAR PENGESAHAN ii

LEMBAR PERNYATAAN..... iii

KATA PENGANTAR.....iv

UCAPAN TERIMA KASIH v

ABSTRAKvi

***ABTRACT*vii**

DAFTAR ISI.....viii

DAFTAR GAMBAR.....xi

DAFTAR TABELxiii

BAB I PENDAHULUAN..... 1

1.1 Latar Belakang..... 1

1.2 Rumusan Masalah 3

1.3 Tujuan Penelitian..... 3

1.4 Batasan Masalah 4

1.5 Manfaat Penelitian..... 4

BAB II LANDASAN TEORI 5

2.1 Teori Dasar Matematika 5

2.1.1 Faktor Persekutuan Terbesar..... 5

2.1.2 Relatif Prima 5

2.1.3 Modulo 5

2.1.4 Grup 5

2.1.5 Ring 6

2.1.6 Lapangan 6

2.2 Teori Dasar Kriptografi 7

2.2.1 Terminologi Istilah..... 7

2.2.2 Kriptosistem 8

2.2.3 Kriptografi Simetri 9

2.2.4 Kriptografi Asimetri..... 9

2.2.5 Teori *Coding* 9

2.3 *Elliptic Curve*..... 11

2.3.1 *Elliptic Curve* pada Bilangan Real 11

2.3.2	<i>Elliptic Curve</i> pada Lapangan Z_p	14
2.3.3	<i>Elliptic Curve Discrete Logarithm Problem</i>	15
2.4	Fungsi Hash	16
2.5	<i>Secure Hash Algorithm 256</i>	17
2.6	Tanda Tangan Digital.....	23
2.7	<i>Elliptic Curve Digital Signature Algorithm</i>	25
2.8	<i>Two-Factor Authentication</i>	26
2.9	Bahasa Pemrograman Python	27
BAB III METODOLOGI PENELITIAN		28
3.1	Identifikasi Masalah	28
3.2	Model Dasar	29
3.2.1	Skema SHA 256.....	29
3.2.2	Skema ECDSA	29
3.2.3	Bagan Alur 2FA	30
3.3	Pengembangan Model.....	31
3.4	Konstruksi Program	31
3.4.1	<i>Input dan Output</i>	31
3.4.2	Algoritma Deskriptif.....	32
3.4.3	Rancangan Tampilan.....	33
3.5	<i>Library Python</i>	34
3.6	Proses Validasi	35
3.7	Pengambilan Kesimpulan.....	36
BAB IV PEMBAHASAN		37
4.1	Rancangan Aplikasi Login Akun dengan ECDSA dan SHA 256	37
4.2	Konstruksi Aplikasi Login Akun dengan ECDSA dan SHA 256	38
4.2.1	<i>Pseudocode</i> Aplikasi Login Akun dengan ECDSA dan SHA 256.....	39
4.2.2	Tampilan Utama	44
4.3	Validasi Aplikasi Login Akun dengan ECDSA dan SHA 256	50
4.3.1	Kasus 1	51
4.3.2	Kasus 2	51
4.3.3	Kasus 3	52
4.3.4	Kasus 4	52
BAB V KESIMPULAN DAN SARAN		54
5.1	Kesimpulan	54

5.2	Saran	55
DAFTAR PUSTAKA		56
LAMPIRAN.....		58

DAFTAR GAMBAR

Gambar 2.1 Tabel ASCII.....	10
Gambar 2.2 Kurva Eliptik $y^2 = x^3 - 4x + 5$	12
Gambar 2.3 Kurva Eliptik $y^2 = x^3 - 4$	12
Gambar 2.4 Penjumlahan Titik Kurva Eliptik.....	12
Gambar 2.5 Penggandaan Titik $y_p \neq 0$	20
Gambar 2.6 Penggandaan Titik $y_p = 0$	20
Gambar 3.1 Skema SHA 256	29
Gambar 3.2 Skema ECDSA	30
Gambar 3.3 Flowchart 2FA.....	30
Gambar 3.4 Skema Program Autentikasi Login Akun.....	31
Gambar 3.5 Tampilan Halaman Pendaftaran Akun	33
Gambar 3.6 Tampilan Halaman Login Akun	33
Gambar 3.7 Tampilan Setelah Memasukkan Username dan Password Benar....	34
Gambar 3.8 Tampilan Login Berhasil	34
Gambar 3.9 Tampilan Login Gagal Karena Username / Password Salah.....	34
Gambar 3.10 Tampilan Login Gagal Karena Kunci Privat Tidak Valid.....	34
Gambar 4.1 Skema Aplikasi Login dengan ECDSA dan SHA 256.....	37
Gambar 4.2 Tampilan halaman menu utama.....	44
Gambar 4.3 Tampilan halaman registrasi akun	45
Gambar 4.4 Tampilan output registrasi dengan kolom kosong.....	45
Gambar 4.5 Tampilan registrasi berhasil.....	46
Gambar 4.6 Tampilan <i>file txt</i> pada <i>server</i>	46
Gambar 4.7 Tampilan <i>file txt</i> pada <i>client</i>	47
Gambar 4.8 Tampilan registrasi dengan username yang telah terdaftar	47
Gambar 4.9 Tampilan halaman login akun	48
Gambar 4.10 Tampilan output login dengan kolom kosong	48
Gambar 4.11 Tampilan mohon tunggu.....	49
Gambar 4.12 Tampilan login berhasil	49
Gambar 4.13 Tampilan login gagal	50
Gambar 4.14 Tampilan <i>username</i> atau <i>password</i> salah	52

Gambar 4.15	Tampilan <i>file</i> kunci privat tidak ditemukan.....	53
--------------------	--	----

DAFTAR TABEL

Tabel 2.1 Desimal ke Heksadesimal 11

Tabel 2.2 Konstanta SHA 256..... 22

Tabel 3.1 Input dan output program..... 31

Tabel 4.1 Validasi aplikasi 53

DAFTAR PUSTAKA

- Aprilia, T., Pitoyo, B. S., Fauzi, A., Ramadhanti, R. G., Nurazizah, R. D., Wanti, E. T., Nugroho, M. Y., Shawa, B. N. P., & Prasetyo, A. R. (2024). Pengaruh Keamanan Two-Factor Authentication Terhadap Pencurian Data (Cyber Crime) Pada Media Sosial. *Madani: Jurnal Ilmiah Multidisiplin*, 2(5), 449-458. <https://doi.org/10.5281/zenodo.11496678>.
- Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., & Yung, M. (2006). Fourth-Factor Authentication: Somebody You Know. In *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 168-178).
- Burton, D. M. (2011). *Elementary Number Theory* (7th ed.). New York, NY: McGraw-Hill.
- Fitri, H. K. (2022). *Implementasi Algoritma Elliptic Curve Diffie Hellman pada Two Way Challenge-Response Protocol sebagai Protokol Autentikasi User*. (Skripsi). Universitas Pendidikan Indonesia.
- Hankerson, D., Menezes, A., & Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography*. New York: Springer.
- Herstein, I. N. (1975). *Topics in Algebra* (2nd ed.). New York: John Wiley & Sons.
- Hutahaean, J. (2014). *Konsep Sistem Informasi* (Ed. 1, Cet. 1). Yogyakarta: Deepublish.
- Judhieputra, R. R., & Anisa, I. N. (2024). *Kriptografi: Penerapan dalam Keamanan Transaksi Komersial*. Indonesia Emas Group.
- Khan, R. R. M. (2023). *Implementasi Elliptic Curve Digital Signature Algorithm dan Algoritma SHA-256 pada Autentikasi RESTful Web API*. (Skripsi). Universitas Pendidikan Indonesia.
- Liao, H. Z., & Shen, Y. Y. (2006). On The Elliptic Curve Digital Signature Algorithm. *Tunghai Science*, 8, 109–126.
- Lutz, M. (2011). *Programming Python* (4th ed.). Sebastopol, CA: O'Reilly Media.

- Munir, R. (2019). KRIPTOGRAFI. Bandung: Informatika Bandung.
- Pardosi, A. G. (2023). *Implementasi Algoritma Elliptic Curve Digital Signature dalam Peningkatan Keamanan JWT* (Makalah Tugas IF4020 Kriptografi, Semester II Tahun 2023/2024). Institut Teknologi Bandung.
- Raharjo, W. S., Ratri, I. D. E. K., & Susilo, H. (2017). Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login. *Jurnal Teknik Informatika dan Sistem Informasi*, 3(1), 127-135.
- Saputra, I., & Nasution, S. D. (2019). Analisa Algoritma SHA-256 Untuk Mendeteksi Orisinalitas Citra Digital. *Prosiding Seminar Nasional Riset Information Science (SENARIS)*, 164-178.
- Srinath, K. R. (2017). Python—The Fastest Growing Programming Language. *International Research Journal of Engineering and Technology (IRJET)*, 4(12), 354-357.
- Stinson, D. R., & Paterson, M. B. (2019). *Cryptography Theory and Practice Fourth Edition*. Boca Raton, FL: CRC Press.