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

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. 196808231994320002

Pembimbing II

Dra. Hj. Rini Marwati, M.S.

NIP.196606251990012001

Mengetahui,

Ketua Program Studi Matematika

Dr. Kartika Yulianti, M.Si.

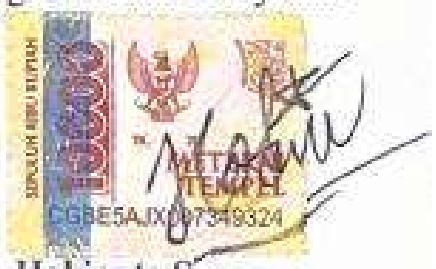
NIP. 198207282005012001

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



Hokianto Suseno

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 Universitasi 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

DAFTAR GAMBAR

DAFTAR TABEL

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.