SKRIPSI

IMPLEMENTASI ECDSA UNTUK AUTENTIKASI DOKUMEN DIGITAL

ECDSA IMPLEMENTATION FOR DIGITAL DOCUMENTS AUTHENTICATION

IBNI MAULANA BINTANG

24010120130114

DEPARTEMEN MATEMATIKA

FAKULTAS SAINS DAN MATEMATIKA

UNIVERSITAS DIPONEGORO

SEMARANG

2024

SKRIPSI

IMPLEMENTASI ECDSA UNTUK AUTENTIKASI DOKUMEN DIGITAL

ECDSA IMPLEMENTATION FOR DIGITAL DOCUMENTS AUTHENTICATION

Diajukan untuk memenuhi salah satu syarat memperoleh derajat
Sarjana Matematika (S.Mat.)

IBNI MAULANA BINTANG
24010120130114

DEPARTEMEN MATEMATIKA

FAKULTAS SAINS DAN MATEMATIKA

UNIVERSITAS DIPONEGORO

SEMARANG

2024

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI ECDSA UNTUK AUTENTIKASI DOKUMEN DIGITAL

Telah dipersiapkan dan disusun oleh :

IBNI MAULANA BINTANG

24010120130114

Telah dipertahankan di depan Tim Penguji

Pada tanggal 7 Februari 2024

Susunan Tim Penguji

Pembimbing II/Penguji,	Penguji,
Zani Anjani Rafsanjani HSM. S.Si., M.Sc.	Drs. Bayu Suraso , M.Sc., Ph.D.
NIP. H.7.199403062022102001	NIP. 196311051988031001

Mengetahui,

Ketua Departemen Matematika,	Pembimbing I/Penguji,
Dr. Susilo Hariyanto, S. Si., M.Si.	Dr. Drs. Kartono, M.Si.
NIP. 19741014200012001	NIP. 196308251990031003

ABSTRAK

IMPLEMENTASI ECDSA UNTUK AUTENTIKASI DOKUMEN DIGITAL

oleh

Ibni Maulana Bintang

24010120130114

Teknologi informasi dan komunikasi (TIK) terus mengalami perkembangan dengan pesat, terlebih untuk kebutuhan transaksi dan pertukaran data digital. Hal ini menimbulkan sejumlah masalah seperti serangan siber yang berdampak pada integritas maupun kerahasiaan data. Penggunaan tanda tangan yang didigitalisasi menggunakan *scanner* pada dokumen – dokumen digital tidak dapat menjamin keautentikan dokumen digital. Berbeda dari tanda tangan fisik yang didigitalisasi dengan scanner, tanda tangan digital dalam kriptografi adalah hasil transformasi kriptografis dari data digital yang menghasilkan mekanisme untuk menguji keautentikan data digital. ECDSA (Elliptic Curve Digital Signature Algorithm) adalah suatu algoritma kriptografi yang digunakan untuk pembuatan tanda tangan digital dengan menggunakan kurva eliptik. ECDSA dipilih dalam penelitian ini karena memiliki tingkat keamanan yang tinggi dan ukuran kunci yang efisien. Oleh karena itu, penelitian ini bertujuan untuk mendalami implementasi Elliptic Curve Digital Signature Algorithm (ECDSA) untuk autentikasi dokumen digital. Penelitian ini mencakup tahap implementasi ECDSA, dimulai dari melakukan proses *hashing* terhadap dokumen masukan, enkripsi *message digest* untuk membuat tanda tangan digital, dan proses verifikasi dengan parameter publik yang disepakati kedua pihak. Penelitian ini menghasilkan skema tanda tangan digital yang dapat memberikan opsi solusi untuk menjaga keautentikan data digital.

Kata kunci: Keamanan data, kriptografi kunci publik, tanda tangan digital, fungsi *hash*, *message digest*, ECDSA

ABSTRACT

ECDSA IMPLEMENTATION FOR DIGITAL DOCUMENTS AUTHENTICATION

by

Ibni Maulana Bintang

24010120130114

Information and Communication Technology (ICT) continues to undergo rapid development, especially for transactions and the exchange of digital data. This resulted a various problems, such as cyber attacks that affect the integrity and confidentiality of data. The use of digitized signatures using scanners on digital documents cannot guarantee the authenticity of digital documents. Unlike physical signatures digitized with a scanner, digital signatures in cryptography are the result of cryptographic transformations of digital data that produce a mechanism to verify the authenticity of digital data. ECDSA (Elliptic Curve Digital Signature Algorithm) is a cryptographic algorithm used for creating digital signatures using elliptic curves. ECDSA was chosen in this research because it offers high security levels and efficient key sizes. Therefore, this research aims to study the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) for digital documents authentication. This research covers the implementation stages of ECDSA, starting from the process of hashing the input document, encrypting the message digest to create a digital signature, and the verification process using agreed-upon public parameters. This research produces a digital signature scheme that can provide optional solutions to maintain the authenticity of digital data.

Keywords: Data security, public key cryptography, digital signature, hash function, message digest, ECDSA