turnitin unesa1

212 Similarity

Turnitin

Document Details

Submission ID
trn:oid:::3618:143518501

Submission Date
Jun 18, 2026, 8:20 PM GMT+7

Download Date
Jun 18, 2026, 8:22 PM GMT+7

File Name
212 Similarity.pdf

File Size
688.4 KB

1 Page

540 Words

3,366 Characters

7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography

Exclusions

- 6 Excluded Matches

Match Groups

3 Not Cited or Quoted 5%
Matches with neither in-text citation nor quotation marks

1 Missing Quotations 1%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

7% Internet sources
3% Publications
0% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **3** Not Cited or Quoted 5%
  Matches with neither in-text citation nor quotation marks
- **1** Missing Quotations 1%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

7% Internet sources
3% Publications
0% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
apsarastackdocument.oss-cn-hangzhou.aliyuncs.com		3%
2	Internet	
www.mdpi.com		2%
3	Internet	
www.grafiati.com		1%
4	Internet	
journal.i-ros.org		<1%

Journal of Current Studies in SDGs
Homepage : https://journal.i-ros.org/index.php/JOCSIS
Email : jocsis@i-ros.org

e-ISSN 3089-7564
Vol.2, No.1, March 2026

Towards Sustainable and Trustworthy Digital Infrastructure: Benchmarking RSA and ECDSA Digital Signature Algorithms in Support of SDGs 9 and 16

Yuliani Puji Astuti*, Ulfa Siti Nuraini

Universitas Negeri Surabaya, Surabaya, Indonesia

Check for updates OPEN ACCESS

DOI : https://doi.org/10.63230/jocsis.2.1.212

Sections Info

Article history:
Submitted: May 21, 2026
Final Revised: June 8, 2026
Accepted: June 8, 2026
First Available Online: June 16, 2026
Publication Date: June 27, 2026

Keywords:
Cryptography;
Digital Signature;
ECDSA;
RSA;
Security.

ABSTRACT

Objective: *This study aims to evaluate and compare the performance of the Rivest–Shamir–Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) digital signature schemes in terms of key generation, signing, verification, and storage efficiency. The research supports the advancement of secure digital communication systems aligned with Sustainable Development Goals (SDGs) 9 and 16, which emphasize innovation, resilient digital infrastructure, and trustworthy institutions.* ***Method:*** *A quantitative experimental approach was employed on a Windows AMD64 platform using Python. Five cryptographic configurations were evaluated: RSA-2048, RSA-4096, ECDSA P-256, ECDSA P-384, and ECDSA P-521. Performance tests were conducted on payload sizes of 1 KB, 10 KB, and 100 KB. Each cryptographic operation, including key generation, signing, and verification, was repeated 100 times to ensure measurement consistency and reliability.* ***Results:*** *The findings indicate that ECDSA significantly outperforms RSA in several performance aspects. ECDSA P-256 reduced signature storage requirements by 72.3%, generated keys nearly 13,000 times faster than RSA-2048, and signed 10 KB payloads approximately 48 times faster. ECDSA P-384 also demonstrated strong performance while providing a higher security level. Although RSA-2048 remains suitable for legacy systems, its efficiency is lower than ECDSA-based alternatives.* ***Novelty:*** *This study provides a comprehensive comparative evaluation of multiple RSA and ECDSA variants across different payload sizes and operational metrics, offering practical recommendations for selecting digital signature algorithms. The results highlight ECDSA P-256 as the optimal choice for 128-bit security requirements and ECDSA P-384 for applications requiring stronger 192-bit security.*

INTRODUCTION

Digital signatures are fundamental components of contemporary cryptographic systems, providing three essential security properties: authenticity, which verifies the identity of the signer; integrity, which ensures that signed data cannot be altered without detection; and non-repudiation, which prevents the signer from denying authorship of the signed document (Gjøsteen & Jager, 2018; Penubadi et al., 2023; Shukla et al., 2022). These properties form the basis of trust in modern digital ecosystems, including electronic commerce, secure communications, software distribution, financial systems, and e-government services (NIST, 2024; Mohammed, 2024).

Among public-key cryptographic schemes, RSA remains one of the most widely recognized and deployed digital signature algorithms (Shah & Gor, 2025; Tanwar & Kumar, 2019). Its security relies on the computational difficulty of factoring large semiprime integers, which continues to be computationally infeasible for sufficiently large key sizes under classical computing assumptions. However, increasing security requirements have resulted in larger modulus sizes, leading to higher computational and storage overheads compared to elliptic-curve-based approaches (Schemitt et al., 2025; Tesoro et al., 2024).