IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, January 2026
Impact Factor: 7.67

A Comparative Study of RSA and ECC Cryptography

Rutuja Y. Bochare and Dr. Pradip D. Pansare
MIT Arts, Commerce and Science College, Alandi, Pune, India
rutujabochare11@gmail.com, pradippansare@gmail.com

Abstract: *Cryptography is a fundamentally critical building block in modern digital security, enabling confidentiality, integrity, authenticity, and non-repudiation across heterogeneous systems. As the world increasingly transitions towards high-density data mobility, cloud computing, and low power Internet-of-Things (IoT) architectures, the selection of an appropriate public key cryptosystem becomes a practical optimisation challenge, not just a theoretical choice. Among the available asymmetric primitives, RSA and Elliptic Curve Cryptography (ECC) are the two most dominant and widely deployed families. However, they rely on very different mathematical hardness assumptions and exhibit significantly different performance characteristics. RSA derives security from the integer factorisation problem, and must inflate key sizes aggressively to maintain equivalent classical security over time. ECC, by contrast, leverages the Elliptic Curve Discrete Logarithm Problem (ECDLP) and therefore achieves strong security with remarkably smaller operand sizes.*

This study presents a comparative academic evaluation of RSA and ECC based on both theoretical constructs and practical Python-based implementation. RSA-2048 and ECC-256 (secp256r1) algorithms were implemented to measure key generation time, encryption and decryption execution time. Output data was not included inside this abstract; the purpose instead is to supply a reproducible mechanism so that final benchmark metrics can be produced directly by the student or examiner during execution. The results in general indicate that ECC demonstrates superior efficiency in key generation and private-key centric operations, whereas RSA remains operationally dominant in legacy PKI infrastructures due to its historical support and standardisation momentum. Overall, ECC proves more suitable for resource-constrained cryptographic deployments such as embedded devices, wireless sensor networks, mobile clients, and blockchain platforms..

Keywords: RSA, Elliptic Curve Cryptography (ECC), Public Key Cryptography, Performance Benchmarking, Python Implementation

DOI: 10.48175/IJARSCT-30961