Abstract

Title: “Fortifying Security through Hybrid Cryptography”

In the ever-changing digital environment, preserving the privacy and reliability of confidential information stands as a top priority. This paper underscores the critical necessity for robust data protection through the introduction of hybrid cryptography, aiming to enhance the security of online communications. The primary objective is to thwart unauthorized access and tampering of data. The study focuses on assessing the efficiency of the proposed approach, particularly in terms of Encryption and Decryption times, as well as key-generation time—vital metrics for overall performance. The strategy advocated combines the cuttingedge Elliptical Curve Cryptography (ECC) with the robust Diffie-Hellman algorithm, both acknowledged for their advanced security features. Through the integration of these sophisticated cryptographic techniques, this research contributes to the ongoing evolution of hybrid encryption methods. Furthermore, it presents a pragmatic solution for reinforcing the security of sensitive data transmitted through communication channels and stored within systems.

Keywords: Diffie-Hellmen, Hybrid Cryptography, Elliptical Curve Cryptography, Key-Generation