AN ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA) FOR SECURING DATA: A CASE STUDY OF PATIENTS' DATA

P. Waruhari[1] and L. Nderu[2]
[1]Department of Electrical and Electronic Engineering, Jomo Kenyatta University of Agriculture and Technology
[2]Department of Computing, Jomo Kenyatta University of Agriculture and Technology
Email: *pwaruhari@jkuat.ac.ke*

Abstract
In this paper, we present the progress of our work in the creation and implementation of an Elliptic Curve Digital Signature Algorithm (ECDSA). We present the design of the algorithm and its implementation in encryption of medical data. ECDSA PHP ECC code has been used to implement the digital signatures over elliptic curve P-256. The work presented highlights practical implementation of ECDSA signature generation to secure and authenticate patient laboratory test results in a Laboratory Information System (LIS). Future work will demonstrate the implementation of decryption using the ECDSA. With the inherent superiority capability of Elliptic Curves (EC) in securing data our algorithm is highly secure and can be adapted in many areas where data privacy and security is paramount.

Key words: Security, encryption, Elliptic Curve Digital Signature Algorithm (ECDSA)