3rd International Conference of Multidisciplinary Approaches (iCMA), 2016
Faculty of Graduate Studies,
University of Sri Jayewardenepura,
Sri Lanka
ISSN: 2386 – 1509

ELLIPTIC CURVE CRYPTOGRAPHY AND CODING THEORY

Sanjeewa R. and Welihinda B.A.K.*

Department of Mathematics, University of Sri Jayewardenepura, Sri Lanka

kasuniwe@gmail.com

ABSTRACT

From the earliest days of history, the requirement for methods of secret communication and protection of information had been present. Cryptography is such an important field of science developed to facilitate secret communication and safeguard information. Cryptography is based on mathematics. It is an application of different disciplines such as Algebra, Number Theory, Graph Theory etc. Private key cryptography and Public key cryptography are the two main types of cryptography. In Private key cryptography a single key is used for both encryption and decryption of messages which renders the inconvenience of having to agree on a common key by the communicating parties prior to the communication. Thus in order to overcome this inconvenience Public key cryptosystems were introduced which involves a pair of keys, namely the Private key and the Public key. Public key cryptosystems offer more security and convenience for the users. The main objective of this study is to explore the possibilities of further improvement of Elliptic Curve Cryptography (ECC) by studying the mathematical aspects behind the "Elliptic Curve cryptosystem" which is one of the latest of this kind and develop a computer program to generate the cyclic subgroup of a given elliptic curve defined over a finite field $\mathbb{Z}$, where is a prime, which is the major requirement to perform ECC and then use the same to illustrate how data security is achieved from this. For an elliptic curve defined over a field, the points on an elliptic curve naturally form an abelian group. Elliptic curve arithmetic can be employed to develop a variety of Elliptic Curve cryptographic schemes such as key exchange, encryption, digital signatures and specific construction of a keyed-Hash Message Authentication Code (HMAC) which are illustrated through this study. Moreover this study proposes an improvement for the encryption of a message through utilization of a concept in "Coding Theory" of Abstract algebra which offers an additional shield for the transmitted message.

Keywords: abelian group, cyclic subgroup, ECDH, ECDSA, AES