Key Generation Based on Elliptic Curve Cryptography

Linn Htaik Kyi, Khin Than Mya

University of Computer Studies, Yangon

linnhtaikkyi@gmail.com

Abstract

In the rapid improvement of communication environment, it is desirable to improve the security measure on the use of between the sender and receiver. Cryptography is an important aspect of communications security and is also a basic building block for computer security. Elliptic curve arithmetic can be used to develop a variety of elliptic curve cryptograph (ECC) schemes, including key exchange, encryption and digital signature. In this paper, we propose a system that provides two users to exchange secret keys securely on an unsecured communication path. ECC is used to exchange a randomly generated conventional encryption key with keyed-hash message authentication code (HMAC) to generate dynamically the secret key. The rest of the exchange is then encrypted message and decrypted message are processed using Advanced Encryption Standard (AES).