Abstract

Since the invention of public-key cryptography, numerous public-key cryptographic systems have been proposed. Each of these systems relies on a difficult mathematical problem for its security. Today, three types of systems, classified according to the mathematical problem on which they are based, are generally considered both secure and efficient. The systems are: the integer factorization systems (of which RSA is the best known example), the discrete logarithm systems (such as the U.S. Government’s DSA), the elliptic curve discrete logarithm systems (also known as elliptic curve cryptosystems).

This paper focuses on implementing cryptographic services with elliptic curve cryptography (ECC). The principle attraction of ECC is that it appears to offer equal security for a far smaller key size, thereby reducing processor overhead. This paper implements Diffie–Hellman Key Aggrement Protocol using Elliptic Curve as the mathematical technique over prime field $F_p$.

Index Terms

Computer Science Software Engineering

Keywords

Diffie-Hellman key Agreement protocol. Elliptic curve cryptography, Elliptic Curve Diffie Hellman(ECDH)