Abstract

The purpose of this research is to enhance the cryptographic system called the Elliptic Curve. Elliptic Curve cryptosystem (ECC) is a technique of public-key encryption, which is rooted on the arithmetical construction of elliptic curves over finite fields. Elliptic Curve Cryptographic System necessitates smaller keys compared to non-ECC cryptography to offer equal security. The security of RSA is based on the computational task of considering extensive numbers leading to an increase in encryption computation time, slower connection of the SSL handshake and increase in CPU usage during handshakes. Therefore, there should be a new way of solving this problem, which is ECC encryption. Elliptic curves are effective for digital signatures, key agreement, generators, pseudo-random and other related tasks. The first phase of the project involves understanding the key exchange of Diffie-Hellman and applying the properties of the Elliptic Curves. It is terminated with key facts that the Elliptic Curve Cryptography has a shorter key length, saves bandwidth, which facilitates key generation during the encryption/decryption of data, also the assurance of faster encryption and decryption, and
notwithstanding its efficiency and efficacy in small devices.

References


Index Terms

Computer Science Security

Keywords

Elliptic Curve Cryptography; Diffie-Hellman; Secured Socket Layer; encryption; decryption; Rivest-Shamir-Adleman; Hypertext transfer protocol; Triple DES; Digital Signature Algorithm.