Abstract

In this paper, we proposed a model for text encryption using elliptic curve cryptography (ECC) for secure transmission of large text and by incorporating the Huffman data compression technique for effective utilization of channel bandwidth and enhancing the security. In this model, every character of text message is transformed into the elliptic curve points \((X_m, Y_m)\), these elliptic curve points are converted into cipher text. The resulting size of cipher text becomes four times of the original text. For minimizing the channel bandwidth requirements, the encrypted text is compressed using the Huffman compression technique in two ways i) x-y co-ordinates of encrypted text and ii) x-co-ordinates of the encrypted text. The resulting system saves the overall bandwidth and further enhances the security.

Reference
Huffman Compression Technique in the Context of ECC for Enhancing the Security and Effective Utilization of Channel Bandwidth for Large Text


- V. Miller, “Uses of elliptic curves in cryptography”, Advances in Cryptology–Crypto '85, Lecture Notes in Computer Science, 218


- Fernandes, A. “Elliptic Curve Cryptography”, Dr.Dobb’s journal, December 1999


- A. Moffat and A. Turpin, "On the implementation of minimum-redundancy prefix codes", 2/4

**Index Terms**

Computer Science Security

**Key words**

Elliptic Curve Cryptography (ECC)
text encryption
Huffman compression