Abstract

Cryptography is an art to protect secret information from attacks. This idea of information security leads to the evolution of cryptography. In this paper, an idea is proposed in which hill cipher is generated with Elliptic Curve Cryptography to provide better security and proper security coverage. Hill Cipher is harder to break due to its linearity and ECC is smaller key size algorithm which provide fast computations as well as memory, speed, bandwidth. ECC provides secure text based cryptography by generating base points on Elliptic curve over the finite field. It starts with plain text conversion by hill cipher then it is converted into its ASCII value to get points on curve and then perform scalar multiplication to encrypt the data and to generate secret and public key. Hill cipher with ECC improves efficiency of cryptography algorithm, provides better security and a level of complexity so that this technique is harder to break.

References

- P. K Sahoo, Dr. Gunamani Jena, Dr. R. K Chhotray, Dr. S. Patnaik, "An implementation of Elliptic Curve Cryptography"; IJERT ISSN: 2278-0181, vol. 2, Issue 1, Jan 2013.
- Oswald, E. (2002), "Introduction to Elliptic Curve Cryptography"; Institute for Applied Information Processing and Communication, Graz University Technology.
- Yuan Xue, "Lectur notes on classical cipher".
- http://www.asciitable.com/

Index Terms

Computer Science
Security

Keywords

Elliptic Curve Cryptography  Hill Cipher  RSA.