Abstract

Internet has become an Integral part and prime need of every human being in their day to day life. People now prefer to do transaction over the internet than doing it offline as it reduces time consumption. In such scenarios, securing customer data is one of the biggest challenges for software developers. For this reason Security protocols like Blind Signature Scheme came into picture where requester is allowed obtain a signature from the signer who signs a message without reading the content of the message, and cannot link the protocol with the resulting
message signature pair. Blind Signature scheme is mostly used for E-commerce applications like Digital payment system, Electronic-voting system as it provides security goals like blindness, untraceability, correctness and nonforgeability. Neal Koblitz and Victor S. Miller has presented Elliptic curve cryptography (ECC) which is an approach to public key cryptography based on algebraic structure of elliptic curves in over finite fields. Elliptic curve cryptosystem is more efficient than other public key cryptosystem due to difficulty in solving elliptic curve discrete logarithm problem. Using the benefits of elliptic curve cryptography we have presented implementation of blind signature scheme using JAVA.

References

- Chwei-Shyong Tsai, Min-Shiang Hwang, Pei-Chen Sung, "Blind Signature Scheme Based on Elliptic Curve Cryptography;" Debasish Jena, Sanjay Kumar Jena and Banshidhar Majhi "A Novel Untraceable Blind Signature Based on Elliptic Curve Discrete Logarithm Problem;" IJCSNS International Journal of Computer Science and Network Security, VOL. 7 No. 6, June 2007
- Fuh-Gwo Jeng, Tzer-Long Chen, Tzer-Shyong Chen &quot;An ECC-Based Blind Signature Scheme;&quot; journal of Networks, VOL. 5, NO. 8, pp. 921-928, August 2010.
- MS. Dhanashree M. Kuthe, Prof. Avinash J. Agrawal &quot;Implementation of Blind
A Novel Proficient Blind Signature Scheme using ECC

- Sumanjit Das and Prasant Sahoo; Cryptoanalysis of signcryption protocols based on Elliptic curve; IJMER, Vol-3, No. 2, Feb 2013.

Index Terms

Computer Science Security

Keywords

Cryptography Digital Signature Blind Signature Elliptic Curve Cryptosystem (ecc) E-cash System.