Abstract

Cryptography and Network Security is one of the most important and emerging research in academic and industry circles. Cryptography usage is a detailed design issue that is largely beyond the scope of the high-level algorithm description earlier. One obvious issue is key size. With many cryptography algorithms, the time it takes to crack a message varies directly with the size of the encryption key. This Research deals with a new cryptographic blinding signature protocol algorithm. The requirements for securing blind signature are privacy, authentication, integrity maintenance and non-repudiation. These are crucial and significant issues in recent times for E-voting which is transacted over the internet through e-commerce channels. A new method of security is suggested which is based on block cipher algorithm.

References

- David A. Santos, Linear Algebra Notes, January 2, 2010 Revision, dsantos@ccp.edu.
- Prakash Kuppuswamy, Dr. C. Chandrasekar, "Enrichment of Security through Cryptographic Public key Algorithm Based on Block cipher", IJCSE, ISSN : 0976-5166 Vol. 2 No. 3 Jun-Jul 2011 PP 347-355.
- Anoop MS, Public Key Cryptography Applications Algorithms and Mathematical Explanations, Tata Elxsi Ltd, India, anoopms@tataelxsi.co.in

Index Terms

Computer Science

Security

Keywords

Public key  Private key  RSA blinding  Chaum's blinding  signing  unblinding
inverse matrix