Abstract

It is widely recognized and accepted that data security will play a crucial and critical role in modern times for businesses will be transacted over the Internet through e-commerce and m-commerce channels. To address these security concerns, various security protocols that are of symmetric-key and asymmetric-key type have been developed. In this paper, we present a hybrid cryptographic system that combines both the symmetric key algorithm, which uses the
A Hybrid Crypto System based on a new Circle- Symmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications

properties of a circle and asymmetric-key algorithm of RSA with CRT. The circle symmetric key algorithm is based on 2-d geometry using property of circle, and circle-centered angle. It is a block cipher technique but has the advantage of producing fixed size encrypted messages all cases. The asymmetric algorithm is RSA with CRT which improves the performance of the basic RSA algorithm by four.

Reference

- Dus and Gupta, Planar geometry (2nd edition)
- The Discrete Logarithm Problem (http://www.cs.toronto.edu/~cvs/dlog/)
- Known-plaintext attack (http://www.tech-faq.com/known-plaintext-attack.shtml)
- Deepak Garg, Seema Verma “Improvement over public Key cryptographic Algorithm” 2009 IEEE International Advance computing conference
- Jinbiao Hou “Research on Database Security of E-Commerce Based on Hybrid Encryption” 2009 International Symposium on Web Information Systems and Applications

Index Terms

Computer Science

Wireless

Key words

Encryption

Decryption

Cryptography
hybrid cryptography

Symmetric Key Algorithms