Abstract

The paper discusses encryption schemes such as public key algorithms (RSA) and One Time Pads. It also discusses various attacks on the RSA algorithm. A brief introduction to Modular Arithmetic, which is the core arithmetic of almost all public key algorithms, has been given. In this paper we propose a variant to the RSA algorithm which is effective against Wiener's Short Secret Exponent attack. The security and the efficiency of the proposed variant have also been discussed.

Reference

Study of RSA and Proposed Variant against Wiener's Attack


Index Terms

Computer Science

Security

Key terms

RSA

one-time

pad

Wiener's attack

modular arithmetic

plaintext

ciphertext