Abstract

This paper presents particle swarm optimization (PSO) method to find the prime factors of a composite number. Integer factorization is a well known NP hard problem and security of many cryptosystem is based on difficulty of integer factorization. A particle swarm optimization algorithm for integer factorization has been devised and tested on different 100 numbers. It has been found that the PSO method performs with little variability over swarm size.

References

Biologically Inspired Computing (NaBIC), 2011 Third World Congress on (pp. 633-640). IEEE.


Index Terms

Computer Science

Algorithms

Keywords

Legendre Congruence    PSO