International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 5, Issue 1, Feb 2015, 117-126
TJPRC Pvt. Ltd.

A FAST FACTORIZATION ALGORITHM FOR COMPOSITE INTEGERS OF THE FORM N = P X Q, WHERE P AND Q ARE PRIMES AND N MOD 6= + 1

NOURELDIEN A. NOURELDIEN & EBTISAM ABAKER

Department of Computer Science, University of Science and Technology, Omdurman, Sudan

ABSTRACT

The factorization of integers of the form N = p x q, where p and q are primes is of special interest in cryptography and algebra. It is well known facts that a prime number P is in one o two series; P mod 6 = ±1, and each prime P generate a series of composite numbers of the form N mod 6 = ±1.

Based on the concept of Integer Absolute Position, which define the position of an integer N, where N mod 6 = ±1, within its series as AP (N) = N div 6, we develop a fast factorization algorithm for composite integers of the form N = p x q, where p and q are primes and N mod 6= + 1.

In comparing the developed algorithm with the well known factorization algorithm Pollard Rho, the developed algorithm out performs Pollard Rho under certain conditions, namely, when the value of the smallest factor p/q is small or when the values of p and q are relatively close.

KEYWORDS: Form N = P X Q, Where P and Q are Primes and N MOD 6= + 1, Cryptography and Algebra