International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 2, Apr 2014, 177-184

A NEW MODULO n MULTIPLICATION ALGORITHM WITH MODERATE FACTORS OF (2n+2) And (2n+6)

A. UMA MAHESWARI & PRABHA DURAIRAJ

Associate Professor, Quaid-E-Millath Government College for Women (Autonomous),
Chennai, Tamil Nadu, India

ABSTRACT

Security is an important technique for many applications including private networks, e-commerce and secure internet access. Public key cryptosystems like the RSA cryptosystem and the El-Gamal cryptosystem are popular security techniques. These cryptosystems have to perform modular exponentiation with large exponent and modulus for security considerations. Modular exponentiation is performed by repeated modular multiplications. This paper proposes an improvised algorithm for modulo n multiplication, where n is odd.

- The remainder with modulus n is derived from the remainders with modulus (2n+2) and (2n+6)
- (2n+2) and (2n+6) can be decomposed into products of relatively prime factors even if n is prime or difficult to be factorized into prime factors.

The efficiency of the proposed algorith is estimated. On comparing the computational complexitiy with the conventional method, the new improvised algorithm is more efficient.

KEYWORDS: RSA Cryptosystem, El-Gamal Cryptosystem, Modular Multiplication, Chinese Remainder Theorem