Abstract

In this paper, we present an algorithm for Residue Number System (RNS) implementation of RSA cryptography based on an existing RNS division algorithm. The proposed algorithm and that of the state of the art were written in C++ programming language to compare their efficiency with respect to execution time. Experimental results show that our algorithm can encrypt and decrypt text without loss of inherent information and faster than the state of the art. It also offers firm resistance to Brute-force and key sensitivity attacks. Considering the moduli-set \{2, 3, 5\} experimental results shows that, our proposed algorithm is 7.29\% and 15.51\%, faster than the state of the art algorithm for integer and non-integer quotients respectively. Also, for the moduli-set \{7, 9, 11\}, our algorithm is as well 11.29\% and 10.36\% faster than that of the state of the art algorithm for integer and non-integer quotient respectively. We carried out an error analysis of the experimental results at 95 degrees significance level.
10. Mansoureh and Mohammed (2012). Non iterative RNS division Algorithm, IMECS Vol. I. ISSN;2078-0966 online

Index Terms

Computer Science Security
Keywords

RSA, RNS, Cryptography, key, algorithm