Abstract

Information security is a critical issue in data communication networks. This is more important in wireless communications due to the fact that the transmitted signal could go beyond the communicating participants. Any person with the right equipment could intercept the transmitted information with ease. It is therefore paramount to encrypt information before transmission to prevent intruders from making meaning to intercepted signals.

In this paper, an improved Rivest Shamir Adleman (RSA) cryptosystem based on Residue Number System (RNS) is implemented. There are two stages of encryption. The first stage is the traditional RSA and the second stage is to further encrypt the cypher text obtained from RSA using smaller moduli. The first stage of the decryption process is to obtain a partial result through Mixed Radix Conversion (MRC). The final stage of decryption is the RSA decryption process. This is to allow a message $m$, for which $m^{e_1}$
Mixed Radix Conversion based RSA Encryption System

References

6. K. A. Gbolagade, An Efficient MRC based RNS-to-Binary Converter for the moduli set, \{22n+1-1, 2n, 22n-1\}. AIMS SA, 2011
9. Edem K. Bankas, Kazeem A. Gbolagade, A New Efficient RNS Reverse Converter for the 4-Moduli Set, \{2n, 2n + 1, 2n – 1, 22n+1 – 1\}, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:8, No:2, 2014

Index Terms

Computer Science

Information Sciences

Keywords

Information Security, Encryption, RSA, RNS, MRC, Forward Conversion, Backward Conversion