International Journal of Theoretical and Applied Physics (IJTAP),
ISSN: 2250-0634, Vol.2, No. I (June 2012), pp. 73-80

# SECRET SHARING METHODS BASED ON RESIDUE NUMBER SYSTEM

**B. KRISHNA GANDHI[a] AND S. SRI LAKSHMI[b]**

[a] Former Vice Chancellor, J.N.T.U., Anantapur, India.

[b] Research Scholar, Department of Mathematics, J.N.T.U(A)College of Engineering, Anantapur, India

## Abstract

Cryptography is the art and science of keeping message secure, has a long and fascinating history. Over the centuries, an elaborate set of protocols and mechanisms has been created to deal with information security issues, when the information is conveyed by physical documents. Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abidance of laws to achieve the desired result. A secret sharing scheme is a method of distributing a message in parts among participants, each of which is allocated a share of the message. The message can be accessed completely only when the group of participants comes together, thus ensuring the safety of the message. We have been using one radix to represent the number system. Recently Residue Number System (RNS) is being applied in cryptography. In RNS A *base* is chosen consisting of a set of relatively-prime numbers. Each normal integer is represented in the RNS as a set of *digits*; each digit is the number's value modulo each of the relatively-prime numbers in the base. In the present paper, new secret sharing schemes are proposed using RNS.

---

**Keywords:** Residue Number System, modules , Cryptography, Secret sharing schemes.