J. of Ramanujan Society of Mathematics and Mathematical Sciences
Vol. 12, No. 1 (2024), pp. 127-136

DOI: 10.56827/JRSMMS.2024.1201.11 **ISSN (Online): 2582-5461**

ISSN (Print): 2319-1023

ENHANCING COMMUNICATION SECURITY: A PRIVATE KEY CRYPTOSYSTEM EMPLOYING THE CHINESE REMAINDER THEOREM

Nagabharana N., L. Praveen Kumar and L. Jyotsna

Department of Mathematical and Computational Sciences,
Sri Sathya Sai University for Human Excellence,
Kalaburagi, Karnataka, INDIA

E-mail : nagabharana@sssuhe.ac.in, praveen.l@sssuhe.ac.in,
jyotsna.l@sssuhe.ac.in

(**Received:** *Aug. 30, 2024* **Accepted:** *Dec. 25, 2024* **Published:** *Dec. 30, 2024)*

Abstract: This paper presents a new private key cryptosystem utilizing the Chinese Remainder Theorem (CRT) for encryption and decryption. The system generates keys by selecting a specified number of distinct primes and a random integer 'a', which is chosen as a random number greater than all the selected primes and coprime to them, ensuring security without revealing the modulus. Encryption and decryption operations are performed within the modulus of each prime, enhancing data protection. The system's security relies solely on the integrity of prime numbers and the randomness of 'a', offering a promising solution for secure symmetric key cryptography.

Keywords and Phrases: Private key Cryptosystem, Modular arithmetic, Chinese remainder theorem and confidentiality.

2020 Mathematics Subject Classification: 11T71, 94A60.

1. Introduction

In the digital age, secure communication is paramount, driving the increasing importance of cryptography [8]. Cryptography, the art of sending messages in disguised form, plays a pivotal role in ensuring the confidentiality and integrity of