ISSN: 1391-8796
Proceedings of 8th Ruhuna International Science & Technology Conference
University of Ruhuna, Matara, Sri Lanka
February 17, 2021

A Novel Cryptosystem using continued fractions

Chathurangi H. M. M.[1], Ranasinghe P. G. R. S.[1*]

[1]*Department of Mathematics, Faculty of Science, University of Peradeniya, Sri Lanka*

The need for secure communication is something that is of paramount importance. Cryptography is the practice and study of techniques for secure communication in the presence of adversaries. Over the years, many researchers developed symmetric and asymmetric key cryptosystems using different approaches to gain higher security than the existing algorithms. In the present work, we introduce a new symmetric key cryptosystem to communicate securely among n number of users. Although most symmetric key cryptosystems are based on block cipher and stream cipher systems, this method is different, as we use a technique similar to the RSA cryptosystem for the encryption process and decryption process. First, an n number of users should agree on two large primes p and q, and each of them should share a key through a private information link. Then the key generation of the proposed algorithm is developed using continued fraction method with these shared keys. In addition, each user must compute encryption keys and decryption keys and both these keys are not shared with the private information link as an advantage. The encryption process and decryption process are done by using developed modular exponentiation. The double encryption process makes the encrypted message large making it difficult to find the corresponding keys to the adversary. Furthermore, the proposed algorithm is more efficient, because the user can identify if there is any man-in-the-middle attack as a security analysis.

Key words: *Block cipher, Stream cipher, RSA cryptosystem, Continued Fraction, Man-in-the-middle attack*

*Corresponding author: rajithamath@sci.pdn.ac.lk