Abstract No: 125 ***ICT, Mathematics, and Statistics***

NOVEL IMPROVEMENT IN RSA ALGORITHM

H.M.M. Chathurangi, A.P. Madhushani and P.G.R.S. Ranasinghe*

Department of Mathematics, Faculty of Science, University of Peradeniya, Peradeniya, Sri Lanka
**rajithamath@sci.pdn.ac.lk*

In 1977, Rivest, Shamir, and Adelman proposed a new public key cryptosystem known to the world now as the RSA algorithm. This system has become one of the acclaimed members of the cryptography family due to its secure and hard to break cornerstone, the factoring problem. However, many researchers are proposing new variants of the original RSA algorithm to overcome its drawbacks. In this study, we propose a new cryptographic scheme based on the textbook RSA algorithm associating the concept of continued fractions. The algorithm was designed under the three primary steps of key generation, encryption, and decryption. The key generation of the system is improved to generate a large encryption key without affecting the decryption key. In this new scheme, the string of plaintexts to be encrypted was taken as a partial quotient of a finite continued fraction representation and the corresponding rational number was calculated. The denominator and the numerator of the rational number should be in their lowest forms. Continued fractions give an additional advantage as it encrypts a string of plaintexts by encrypting only two integers optimising the time and the memory consumption. The encryption and the decryption processes are similar to that of the standard RSA algorithm; insomuch the implemented algorithm does not affect the security of the RSA algorithm, which depends on the factoring problem. In addition, as the algorithm uses a large encryption key, it has been proven that the system is secure against Wiener's attack.

Keywords: Continued fraction, Factoring problem, RSA Cryptosystem, Wiener's attack