A VARIANT OF RSA ALGORITHM WITH USE OF FERMAT'S LITTLE THEOREM

H.M.M. Chathurangi and **P.G.R.S. Ranasinghe***

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

In cryptography, symmetric and asymmetric cryptosystems are the two basic types. Although an asymmetric cryptosystem has two keys, namely public and private, a symmetric cryptosystem has only one key. One of the well-celebrated asymmetric cryptosystems is the RSA cryptosystem, founded in 1976 by Ron Rivest, Adi Shamir, and Leonard Adleman. Considering the variants of RSA, the use of multi-prime numbers increases the strength of security because it makes the factorization of the modulus more difficult. So, the multi-power RSA system is more secure than the original RSA. Hybrid cryptography is one which combines the asymmetric key cryptosystem and the symmetric key cryptosystem. It combines the benefits of both algorithms. In this study, we introduce a hybrid cryptosystem based on multi-power RSA system and Fermat's Little Theorem. We have used a symmetric key which is generated by the sender and an asymmetric key which is generated by the receiver. Hence, the key generation of the proposed algorithm is performed by both parties, and the security of the new method is guaranteed by the multi-power modulus and key generation.

Keywords: Fermat's Little Theorem, Hybrid cryptosystem, Multi power RSA cryptosystem, RSA cryptosystem