Compression-RSA: New Approach Of Encryption And Decryption Method

ABSTRACT

Rivest-Shamir-Adleman (RSA) cryptosystem is a well known asymmetric cryptosystem and it has been applied in a very wide area. Many researches with different approaches have been carried out in order to improve the security and performance of RSA cryptosystem. The enhancement of the performance of RSA cryptosystem is our main interest. In this paper, we propose a new method to increase the efficiency of RSA by shortening the number of plaintext before it goes under encryption process without affecting the original content of the plaintext. Concept of simple Continued Fraction and the new special relationship between it and Euclidean Algorithm have been applied on this newly proposed method. By reducing the number of plaintext-ciphertext, the encryption-decryption processes of a secret message can be accelerated.