Information and Management Sciences
Vol. 6, No. 3, pp.1-11, 1995

Cryptanalysis of a Cryptographic System Based upon the Continued Fraction

Wei-Bin Lee
National Chung Cheng University
R.O.C.

Chin-Chen Chang
National Chung Cheng University
R.O.C.

Abstract

In 1993, Jan and Kowng proposed a cryptographic system based on the continued fraction. In their system, to encipher and to decipher only needs some simple multiplications and additions. Therefore, the scheme is efficient in enciphering and deciphering. Yet, in this paper, we will show that Jan and Kowng's scheme cannot withstand the chosen plaintext and known plaintext attacks.

Keywords: Continued Fraction, Chosen Plaintext Attack, Known Plaintext Attack.