Malaysian Journal of Mathematical Sciences **1(1)**: 63 - 81 (2007)

The Quartic Analog to the RSA Cryptosystem

Wong Tze Jin, Mohamad Rushdan Md. Said,
Kamel Ariffin Mohd. Atan & Bekbaev Ural
Institute for Mathematical Research, Universiti Putra Malaysia,
43400 UPM, Serdang, Selangor, Malaysia
E-mail : tjwong1979@gmail.com, mrushdan@fsas.upm.edu.my

ABSTRACT

This paper reports an investigation into a public key cryptosystem, which is derived from a fourth order linear recurrence relation and is based on the Lucas function. This cryptosystem is also analogous to the RSA, LUC and LUC_3 cryptosystems. The explicit formulation involves a generalisation of the Euler Totient function, which underlie the algebra of the RSA cryptosystem.

Keywords: Quartic Polynomial, Resolvent Cubic Polynomial,Fourth Order Lucas Sequence, Sixth Order Lucas Sequence, Euler Totient Function, Quartic Cryptosystem