On the variants of RSA cryptosystem and its related algebraic cryptanalysis

ABSTRACT

The RSA cryptosystem is the earliest public key cryptosystem which came into existence since 1978 and has become the most broadly used public key cryptosystem in the world. So far, RSA is being implemented as a default cryptosystem in most of web browsers and also most commonly used feature to secure internet banking systems. For decades, studies on improving the efficiency of RSA in terms of its encryption and decryp-tion time, and also its security were conducted. Hence, many variants of RSA were proposed to overcome such said issues. Essentially this review article attempts to analyze the variants of RSA cryptosystem which shared a similarity of possessing its public key e and private key d satisfying this particular key equation of the form ed − k(p 2 − 1)(q 2 − 1) = 1 where the product of (p 2 − 1)(q 2 − 1) is referred as modified Euler totient function. This review article also emphasizes on the algebraic cryptanaly-sis methods proposed on those variants cryptosystems specifically via the continued fractions method and the lattice reduction method.

Keyword: Variants of RSA; Algebraic cryptanalysis; Continued fractions method; Lattice reduction method.