Abstract No: 28 ***ICT, Mathematics, and Statistics***

NOVEL VARIATION OF THE RABIN CRYPTOSYSTEM USING CONTINUED FRACTIONS

S.N.B.M.C.M. Nawarathna* and P.G.R.S. Ranasinghe

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

Cryptography is the process of concealing information and communications so that only the intended recipient can read it. It involves the use of complex algorithms and computational techniques to transform original data into unreadable forms, ensuring its confidentiality. The Rabin Cryptosystem is one of the widely known public key cryptosystems and its security depends on the inherent difficulty of integer factorization, mirroring the RSA cryptosystem. Two large prime numbers are selected as private keys, and their product serves as the public key. A message is encrypted by squaring and decrypted by computing the square roots modulo the composite number generated by the two primes. A variant known as the H-Rabin Cryptosystem incorporates a third prime number for enhanced security. In both the Rabin and H-Rabin Cryptosystems, the chosen prime numbers share a congruence of 3 modulo 4. In the present study, the key generation was developed using three odd primes and continued fraction representations of random positive integers. This modified public key cryptosystem employs the product of any three odd primes $p, q,$ and r as n and another key e_a with the continued fraction representation for its public key, with private key as p, q, r and multiplicative inverse of e_a modulo n. In the encryption, the plaintext converts into binary form to ensure that the message can be represented in a numerical form suitable for mathematical operations. Bits were replicated to increase the security of the encryption process. After converting it into the decimal form, the message was encrypted by squaring modulo, the product of the three odd primes. The decryption process is based on the Chinese Remainder Theorem and the Tonelli-Shanks Algorithm to find the square roots modulo that composite number. In the Rabin cryptosystem, solving the quadratic residue of the ciphertext yields four distinct solutions. Both the H-Rabin cryptosystem and our proposed algorithm produce eight different outputs, necessitating the identification of the original message among these possibilities. A replication technique that was used during encryption was applied to identify the correct plaintext. A polynomial-time Las Vegas algorithm RANDOM-FACTOR with the BREAK-RABIN oracle to factor composite numbers efficiently, reducing the likelihood of successful factoring and strengthening the overall cryptographic security.

Keywords: Chinese Remainder Theorem, Continued fractions, Integer factorization, Rabin cryptosystem, Tonelli-Shanks algorithm