Abstract No: 225 ***ICT, Mathematics & Statistics***

A NOVEL CRYPTOGRAPHIC SCHEME BASED ON THE COLLATZ CONJECTURE

R.M.V.V. Bandara* and P.G.R.S. Ranasinghe

Department of Mathematics, University of Peradeniya, Peradeniya, Sri Lanka
**s16322@sci.pdn.ac.lk*

The Collatz conjecture is one of the most famous unsolved problems in mathematics, which is named after the mathematician Lothar Collatz, who introduced the idea in 1937. The Collatz function is defined for any positive integer n; if n is even, then divide it by two; else, multiply it by three and add one. We can modify this function by writing the even number of the form $k \cdot 2^m$ for an odd number k and some positive integer m. The Collatz sequence is generated using this function, and the next term of the sequence is obtained by applying the function to the previous term. In the present cryptographic scheme, we use the Collatz sequence to encrypt a plaintext symmetrically. We have proposed a new cryptosystem in which the sender and the receiver hold the secret key pair (k, n); for some large, odd numbers k and some positive integer n. The key pair has been chosen randomly, and plaintext is encrypted using the Collatz sequence generated starting with k and n number of iterations in the generated sequence. The Collatz sequence is a chaos-based sequence, and for every positive integer, there is a unique mapping, and a slight change in the number makes a huge difference in the generated sequence. Thus, the chaotic nature makes it more secure. Furthermore, this cryptosystem has uncomplicated transformations, which are very simple to analyse and efficient because the only operations involved are multiplication and addition. The present cryptosystem suggests only encrypting the plaintext once, but we can encrypt the plaintext a finite number of times to make it more secure. Also, we can combine this method with some known cryptosystems to implement novel cryptosystems.

Keywords: Chaotic Nature, Collatz Sequence**,** Cryptography