Abstract No: PO-24 **Physical Sciences**

A masking method for resisting key attacks on AES

P. S. L. Perera* **and G. S. Wijesiri**

Department of Mathematics, Faculty of Science,
University of Kelaniya, Sri Lanka
saumyaperera123@yahoo.com

Cryptography is the science of securing data. It makes us easy to store sensitive data and transmit across insecure networks. Modern cryptography is applied in smart cards, computer passwords, and electronic commerce.

Data Encryption Standard (DES) was a popular symmetric-key (64-bit) block cipher in USA from 1970's. It was broken in 1999 by making the key length insecure with the improved computer speed. Later AES (Advanced Encryption Standard) was introduced to replace DES. Both key expansion and encryption algorithms of AES depend on S-boxes and calculations are done on the finite field GF (2^8). AES uses substitution-permutation and 128 block size while DES uses a balanced *fiestel* structure and 64 block size. DES has already broken but AES is still in use and is not completely broken. Today, key attacks for AES are steadily in progress. Since AES has theoretically broken by some key attacks, it is already at a risk of practical breakthrough. Algebraic attacks and related- key attacks are two of the main key attacks. The objective of the algebraic attack is recovering the key by solving system of multivariate polynomial equations over a Galois field. Related-key attacks use multiple pairs of plaintexts and encrypt each of them using two keys. As a result, the encryption key can be recovered.

In this paper, we are going to combine AES algorithm with DNA cryptography which is a branch of Nano-cryptography to enhance the security of AES. We propose an improved algorithm to provide security against key attacks. In the algorithm we use masking techniques and DNA cryptosystem concepts based on the *Vigenere* cipher. DNA cryptography concepts help to avoid the weaknesses of *Vigenere* cipher and provide both computational and biological security.

Keywords: Symmetric-key cryptography, DNA cryptography, Vigenere cipher