DEVELOPING A NEW ROBUST PRIVATE KEY ENCRYPTION ALGORITHM

Prepared by: Lee Kah Hui

ABSTRACT

The objective of this project is to develop a new encryption algorithm that applies key hopping, variable key length and algorithm hopping that differs from conventional cryptographic algorithms. The algorithm is based on a symmetric block cipher. A plaintext is divided into variable length data blocks and each block is equipped with a unique sub-key. The sub-keys are extracted from a master key and a sub-key is having the same length as the data block. There are 64 algorithms that defined the encryption sequence. Each data block is processed using one of the algorithms. The performance and strength of new algorithm is expected to be better than conventional cryptographic algorithm and highly effective against brute force attack. A windows application is implemented in order to illustrate and test the performance and robustness of the new encryption algorithm.