ABSTRACT

Information and communications systems today transmit vital information. The Internet has brought fundamental changes to the world. Information is vulnerable to threats from unauthorized access and use and there is a tremendous potential for fraud in the electronic world. The ability to make multiple copies and undetectable alterations of digitized data complicates the issue further. Cryptography is the fundamental technology implemented for providing security to computer networks. It is applied to ensure authenticity and integrity of documents transmitted electronically. Cryptography also offers challenges to the research community by raising new questions not addressed by researchers and developers. This thesis studies logics of knowledge and cryptography. Specifically, the thesis addresses the problem of how to make the concept of knowledge reflect feasible computability within symmetric cryptography. Digital money systems use cryptography to create a unique electronic representation. This thesis work introduces the notion of “Secure Transmissions” on the internet and discusses several kinds of “Network Interruptions” that breach security, thus defeating the purpose of Cryptography. Requirements for “Secure Algorithms” to minimize network Interceptions are also suggested. Cryptography is based on implementing complex algorithms. A comparative study of symmetric encryption algorithms are presented in this thesis. Since generation of the Secret key is an important aspect of symmetric encryption, a new method is proposed for generating secret symmetric keys based on a co-operative key simulation model with participation from the sender and receiver. A new and powerful algorithm CKE is introduced and its advantages presented. Since CKE uses a secret key, it enjoys the benefits of the private key cryptography joining two 64-bit keys together for generating a single 128-bit key.
Organizations need security mechanisms that provide confidentiality for outsourcing their data services. Encrypting sensitive data is the normal approach in such a situation. Encryption is done to provide confidentiality of information and preventing the messages from the public. Nonlinear functions of a cipher are the main source of cryptographic strength and much research has been done in the area. This research work introduces a new block cipher algorithm called New Dimension Peer to Peer Encryption (NDPPE). NDPPE adopts the basic concepts of Feistel Ciphers with a variable 256 bit secret key. Most importantly NDPPE uses the senders email id for creating this secret key. Existing schemes with multi signers impose requirements that make them impractical. This research work proposes a new encryption scheme called Multi-party Supportive Symmetric Encryption (MSSE) where each authorized user’s information is used to encrypt and decrypt data. This thesis work takes an effort to resolve the security issues and also report on the results of the implementation. The efficiency of the algorithms are also proved on a mathematical basis. The main contributions are as follows.

- Generalized solutions for transmissions on the network, specifically the do’s and don’ts.
- A new Algorithm CKE on a co-operative key simulation model.
- Advanced aspects in Secret key generation.
- A new Algorithm NDPPE involving the participating parties information in key generation.
- The thesis finally delivers a new and efficient block cipher in MSSE.