CONCLUSION

Internet systems suffer from interceptions and capturing traffic is a requisite of any monitoring system. Considerable research has focused on preventing attacks and improving security. Though encryption techniques provide an unbreakable barrier to information, a determined attacker with moderate resources can decrypt the information. The challenge is threefold. First challenge is developing and implementing the technology. The second one is planning for the failures in technology and finally it should be ensured that the public understand and use this technology. Interceptions are possible and confidence in the relationship between an individual and entity is necessary. Standardization is an important factor as law and industry need to work together and provide the architecture and standards. Messages encrypted in cryptographic systems can be measured by the number of bits they contain.

This research work has suggested improvements in creating and maintaining the keys as key generation forms an important part of encryption. Further, the thesis has demonstrated a new algorithm and method of encryption and decryption using a mathematical technique in CKE. It is useful for the refinement of the cipher text to increase the complexity to produce the better cipher text. The refinement process may be continued to give next better cipher text. As the method is dependent on multiple symmetric keys established by a newer mathematical algorithm and to the best of our knowledge it would be difficult to attackers for cryptanalysis.

Block Cipher algorithms are extremely important to Communication Security. Block Cipher algorithms are extremely simple to
implement, relative to some asymmetric algorithms. Block Cipher algorithms also have the advantage that it is not difficult to encrypt and decrypt messages, because the same key is used to encrypt and decrypt. This is in comparison to asymmetric algorithms in which one has a separate public key and is necessary for every person to maintain secure transmissions. The convenience, ease of use, and relatively secure algorithms are what make Block Cipher algorithms a good choice for Communication Security. The proposed block cipher algorithm NDPPE enhances the diffusion. This enhancement is developed to increase the key complexity as a measure against attackers where the attacker takes more time to achieve the analytical process. NDPPE can be implemented as software by simplifying the operations.

The research work explores further in presenting new data encryption scheme (MSSE) that does not require a trusted data server. Unlike previous searchable data encryption schemes that require a shared key for multi-user access, each user in our system has a unique set of keys. The data encrypted by one user can be correctly decrypted by all the authorized users in the system. Moreover the keys can be easily revoked without any overhead, i.e. without having to re-encrypt the stored data.

BIBLIOGRAPHY