Abstract No: 296 ***ICT, Mathematics and Statistics***

ENCRYPTION ALGORITHMS USING GRAPH THEORY IN SYMMETRIC CRYPTOGRAPHY FOR PROVIDING BETTER DATA SECURITY

P.A.S.D. Perera* and G.S.Wijesiri

Department of Mathematics, Faculty of Science, University of Kelaniya, Kelaniya, Sri Lanka
**dhanalishalini@gmail.com*

Web and network technologies are growing rapidly; hence, the most common challenge is to protect the information exchanged over the web or other types of media. Cryptography is one of the focused areas of cyber security which converts information from its natural form to an incomprehensible form. Symmetric and asymmetric cryptography are the two main branches of cryptography. Since the graphs can be represented by matrices, and can be converted into images, graph theory is widely applied in cryptographic algorithms. Throughout this research, an algorithm is proposed to build an important relationship between graph theory and symmetric cryptography, and to develop a code for the proposed algorithm, to store and transmit data in a particular form so that only for those whom it is intended can read and process it. In these proposed methodologies, the original texts are converted into graphs and then represented those as matrices. All proposed algorithms produce ciphertexts which are larger than the plaintext size. Also, these algorithms perform n^3number of operations if the plaintext is of size n. Time complexity is computed using Big-Oh notation. Further, some additional edges are added to the graphs generated by the third algorithm which it performs an equal number of operations as in the other two proposed algorithms. Therefore, when security is considered, the third proposed algorithm is more powerful than the other two. However, when storage is considered, the second proposed algorithm is better than the other two as it produces a single matrix as the ciphertext.

Keywords: Decryption, Encryption, Graph theory, Symmetric key cryptography