A Block Cipher Using Graph Structures and Logical XOR Operation

Abstract

Cryptography is the science of making and breaking the secret communications. Due to widespread use of internet in modern times virtually every computer in the world is connected to every other computer. So, there is a threat of hacking and stealing of the message. In general cryptographic primitives are designed to satisfy particular security objectives which may be built...
from the basic features of confidentiality and authentication. In the present paper a new block cipher encryption is proposed using adjacency matrix of undirected graph structures. In addition logical XOR operation is technically applied to get a good avalanche effect which is one of the desired properties of a good encryption algorithm.

Reference


Index Terms

Computer Science Security
Key words

Adjacency matrix  Logical XOR operation

Decryption.

Encryption