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...
A Block Cipher Using Graph Structures and Logical XOR Operation

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

- Amos Beimel, Tal Malkin, Kobbi Nissim and Enav Weinreb, “How should we solve
- Anna M. Johnston, Peter S. Gemmell, “Authenticated key exchange Provably Secure
- C. Blundo, A. Santis, D.R. Stinson and U. Vaccaro “Graph decompositions and
- Carlisle Aams and Stafford Tavares, “The Structured Design of Cryptographically
- Eli Biham, “Cryptanalysis of multiples modes of operation”, Journal of Cryptology,
- John Blaack and Phillip Rogaway “CBC MACs for Arbitrary-Length Messages: The
- J. Kelesey B. Schneir and D. Wagner, “key-schedule cryptanalysis of
  IDEA,G-DEA,GOST,SAFER and triple-DES. In N. Koblitz editor”, Advances in cryptology-
- B. Krishna Gandhi, A. Chandra Sekhar and PVDG Prasad “Cryptographic
  schemes for digital signals”, IETECH International Journal of Advanced Computations,
- B. Krishna Gandhi, A. Chandra Sekhar and S. Srilakshmi “Cryptographic schemes
  for digital signals using finite state machines”, International Journal of Computer
- Lorenz Minder and Alistair Sinclair, “The Extended k-tree Algorithm” Journal of
  cryptologyDOI: 10.1007/s00145-011-9097-y.
- Steve Lu, Dameil Machala and Rafail Osterousky, “Visual Cryptography using
- Victor Shoup and Rosario Gennaro “Securing Threshold Cryptosystems against
- Yvo Desmedt, Josef Piprzyk, Ron Sternfield, Xiaoming Sun and Tartary, “Graph
  Coloring Applied to Secure Computation in Non-Abilian Groups”, Journal of
  Cryptology, Springer, online from 5th September 2011.

Index Terms

Computer Science Security
Key words

Adjacency matrix
Logical XOR operation

Decryption.

Encryption