Abstract

In this paper we show how implemented one time security encryption scheme is more lucid, effective. However it is more complex in nature of attacker view. The one-time pad encryption scheme itself is mathematically unbreakable. (See Claude Shannon's "Communication Theory of Secrecy Systems"). Therefore, the attacker will focus on breaking the key instead of the cipher text. Random key stream can be used to create lifetime supply of keys for one time pads. Here we provided the practical approach that you can use to set up your own one-time pad encryption. Permutation techniques can be used in conjunction with other technique includes substitution, encryption function etc. for effective performance. The goal of this paper to show how the one-time pad encryption technique can be achieved including complement approach technique.
Reference

- Information Technology Journal 4(3) : 204-221,2005.
- Claude Shannon's "Communication Theory of Secrecy Systems".
- Thomas L. Floyd “Digital Fundamentals”.
- Neal R. Wagner “The Laws of Cryptography: Perfect Cryptography: The One-Time Pad”.
- Pete McCollum “Encryption Via One-Time Pads”.
- Erskine, Ralph, "Enigma’s Security: What the Germans Really Knew", in "Action this Day", edited by Ralph Erskine and Michael Smith,

Index Terms

Computer Science        Security

Key words

Cryptography        One-time pad        Encryption

Key-Enhancement

Network Security

Computer Security