A Block Cipher Generation Using Color Substitution

Abstract

The most powerful and common approach to countering the threats to network / information security is encryption [1]. Even though it is very powerful, the cryptanalysts are very intelligent and they were working day and night to break the ciphers. To make a stronger cipher it is recommended that to use: More stronger and complicated encryption algorithms, Keys with more number of bits (Longer keys), larger block size as input to process, use authentication and confidentiality and secure transmission of keys.

It is for sure that if we follow all the mentioned principles we can make a
very stronger cipher. With this we have the following problems: It is a time consuming process for both encryption and decryption. It is difficult for the crypt analyzer to analyze the problem. Also suffers with the problems in the existing system.

The main objective of this paper is to solve all these problems and to bring the revolution in the Network security with a new substitution technique [3] is 'color substitution technique' and named as a "Play color cipher".

Reference

[6] " for number of colors in the world" www.whyiscolor.org,
[7] " for number of colors in the world" www.jimloy.com
[8] Microsoft visual studio 2008 programming by Jamie
[9] .Net frame work reference by Dan Rahmel

Index Terms

Computer Science
Security

Key words

RSA
EFF:
Electronic frontier foundation

PUB: Public key of user B
PRA: Private Key of user A
PUA: Public key of user A

PRB: Private Key of user B

PCC: Play color cipher.