Abstract

Sometimes the information, which is transferred during the communication, is very much confidential which is needed to be secure. For securing the information various encryption algorithms like DES, BLOWFISH, RC4 etc., are used. Our aim in this paper is to find the two keys using cryptanalysis method, that is used for encrypting the information transferred during communication by using the Meet in the Middle Attack on triple S-DES algorithm, instead of using Brute force attack.

And also we have analysed how the meet in middle attack in S-DES is better than the brute force attack to break the keys in terms of time taken, that is the key search
space is just half in meet in middle. Our analysis can be applied on DES also.

Reference

- [RUPE92] Rueppel, T. "Stream ciphers" IN [SIMM92].
- Nicolas T. Courtois1, Karsten Nohl2, and Sean O'Neil3 1 University College London, UK 2 University of Virginia, USA 3 VEST Corporation, France "Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards" March 2008.

Index Terms

Computer Science  Network Security
Key words

RC4

Stream

Cipher

Block Cipher

Encryption and Decryption