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 are 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
Meet In The Middle Attack: A Cryptanalysis Approach

space is just half in meet in middle. Our analysis can be applied on DES also.

Reference


Index Terms

Computer Science Security
Key words

DES

Meet in the Middle attack

Triple S-DES

Two Key Method

differential and linear cryptanalysis