Abstract

The main feature of Blowfish algorithm is its variable key size (ranges from 32 to 448 bit). The blowfish algorithm is 16 round feistel network and it uses large s-boxes which are key dependant. Blowfish algorithm use value of \( \pi (=3.14159\ldots) \) to calculate the sub key values, but in cryptanalysis it is claimed that if attacker knows the value of hexadecimal digits of \( \pi \) those we used for generation of sub keys, then it is easy for attacker to break key. In this paper random number generator (RNG) is introduced to create a set of values instead of \( \pi \) value. Seed value is kept private so that no one can guess the value of sub keys and the random number generator (RNG) function is declared public. Also the 16 rounds of blowfish are
replaced by 17 complex rounds of IDEA (International data encryption standard) to enhance the security. This paper focuses on enhancing security of Blowfish algorithm for digital content delivery.

References


Index Terms

Computer Science  Security

Keywords

Feistel Network  Cryptanalysis  Random Number Generator.