Strength of Data encryption standard (DES)

Data encryption standard (DES) is a symmetric key block cipher algorithm. The algorithm is based on Feistel network. The algorithm uses a 56-bit key to encrypt data in 64-bit blocks.

There are mainly two categories of concerns about the strength of Data encryption standard. They are:

1. Concerns about the particular algorithm used.
2. Concerns about the usage of key of size 56-bit.

The first concern regarding the algorithm used addresses the possibility of cryptanalysis by making use of the DES algorithm characteristics. A more severe concern is about the length of secret key used. There can be (approximately 7.2 × keys) possible keys with a key length of 56 bits. Thus, a brute force attack appears to be impractical.

Assuming that on an average one must search half the key space, to break the cipher text, a system performing one DES encryption per microsecond might require more than thousand years. But the assumption of one DES encryption per microsecond is too conservative. In July 1998, DES was finally proved to be insecure when the Electronic Frontier Foundation (EFF) had broken a DES encryption. The encryption was broken with the help of a special purpose “DES cracker” machine. It was reported that the attack took less than 3 days.

Simply running through all possible keys won’t result in cracking the DES encryption. Unless known plain text is given, the attacker must be able to differentiate the plain text from other data. Some degree of knowledge about the target plain text and some techniques for automatically distinguishing plain text from garble are required to supplement the brute-force approach. If brute force attack is the only means to crack the DES encryption algorithm, then using longer keys will obviously help us to counter such attacks. An algorithm is guaranteed unbreakable by brute force if a 128- bit key is used.

The differential cryptanalysis, linear cryptanalysis, are examples for statistical attacks on DES algorithm. Few of the important alternatives for DES are AES (Advanced Encryption Standard) and triple DES.