Data Encryption Standard (DES) Algorithm

The article continues the discussion on Algorithms available in Symmetric Key cryptography. It explains the whereabouts of DES algorithm. Due to the limitations of DES on security context, we shall include Triple DES in the scope. Triple DES is a stronger form of DES algorithm.

Understanding Data Encryption Standard (DES)

DES Is a block cipher i.e. it operates on the blocks of plaint text input message. It is a symmetric key encryption scheme i.e. the same secret key is used for encrypting and decrypting message. DES uses a key of bit length 56 bit, which is considered short. And hence DES algorithm is considered weak. Few foundations have proclaimed to break the DES algorithm in 22 hours. DES algorithm takes input plain text bits of fixed length and processes using the key, and transforms the plaintext through a complicated series of operations to produce cipher text (of same length). In actual, the key length for DES key is 64 bits, but only 56 bits are considered and the rest of 8 bits are used as parity bits (for calculating checksum).

DES is considered to be lacking strength for many applications, mainly due to the 56-bit key size being too small. Some critical analysis have theoretically proved the weakness of DES algorithm, although it is practically too tough to crack it.

Triple DES: A stronger form of DES

DES algorithm has another form which is comparatively considered secure – Triple DES. Triple DES algorithm involves key of length 3 X 64 = 192 bits, which is three times the key length of single DES key

A triple DES consists of three DES keys – say k1, k2 and k3 each of 64 bits. In Triple DES encryption, data is encrypted with first key (k1), then the output is decrypted with second key (k2) and then the resultant is again encrypted with third key (k3).

It is important to remember that only 56 bits of each key i.e. k1, k2 and k3 are considered and not 64 bits. That means, 8 bits of every key is ignored as key bits and used as parity bits
Based on the values of these three keys, Triple DES can be categorized into 3 types, also known as keying options –

a. Single key Triple DES

If all the three keys are identical, then it is known as keying option 3.
For example – if your single DES key is abcdef0123456789, then your equivalent Triple DES key would be –
abcdef0123456789 abcdef0123456789 abcdef0123456789
<------k1---------> <------k2---------> <------k3---------->

b. Two key triple DES

If the first and the third keys (i.e k1 and k3) are identical, it is called as keying option 2
For example –
If k1 = abcdef0123456789 and k2 = 9abcdef012345678 , then the equivalent triple DES key would be –
abcdef0123456789 9abcdef012345678 abcdef0123456789
<------k1---------> <------k2---------> <------k3---------->

c. Triple DES

If all the keys are different, then the keying option is 1
For example –
k1 = abcdef0123456789
k2 = 9abcdef012345678
k3 = 89abcdef01234567
Equivalent Triple DES key would be -
abcdef0123456789 9abcdef012345678 abcdef0123456789
<------k1---------> <------k2---------> <------k3---------->

The DES algorithm is now superceded because of its shorter key size, by a much stronger scheme known as Advanced Encryption Standard (AES).

Source: http://www.go4expert.com/articles/data-encryption-standard-des-algorithm-t24538/