Double/Triple DES

Double DES is essentially applying DES twice, with two different keys to the input block:

$C = E(K_2, E(K_1, P))$

P is the plaintext, K_1 is the first key, K_2 is the second key and C is the resulting ciphertext.

To decrypt, we do the following:

$P = D(K_1, D(K_2, C))$

Essentially, we have to undo the transformations in reverse order.

Double DES is more secure than regular DES, though this wasn't formally proven until 1992. In particular, for some combination of keys K_1 and K_2, there is no possible key K_3 that achieves the identical encryption for each possible block as K_1 and K_2 in tandem. This is NOT true for a regular substitution cipher, for example, or a Vigenere cipher with two keywords of the same length. (Notice that mathematically, for both of these examples, the composition of two functions can be represented as a single function of the exact same type.)

One piece of intuitive evidence that this is the case is that the total number of permutations of size 2^{64} (the number of possible functions a DES key could represent) is $(2^{64})!$ and this is much, much larger than the actual number of keys (2^{56}).

Attack on Double DES

If you had a single plaintext, P and corresponding matching ciphertext, C, then you could do the following meet in the middle attack:

For each possible key, K_1, calculate $E(K_1, P)$. **Store** each possible cipher text with its matching key in a huge hash table. (A hash table is a data structure where you can quickly find if an entry with a particular key, in this case the cipher text appears.)

This table would be very large:
C_1 --> K_1
...
C_n --> K_n, where $n = 2^{56}$.

Then, for each possible key K_2, calculate $M = D(K_2, C)$. For each M, see if it belongs to the hash table previously mentioned. If it does, there's very, very high chance that these are the two matching keys. In fact, you could just go through all of the keys and keep a list of all possible pairs (K_1, K_2) that arrive at matching "midpoints" in the process.

Triple DES

In light of the Meet in the Middle Attack, Triple DES was created.

There are multiple versions of this. The most straightforward version just uses 3 separate keys, K_1, K_2 and K_3 for encryption:

$C = E(K_3, E(K_2, E(K_1, P))$

Another version uses just uses two keys, K_1 and K_2 as follows:

$C = E(K_1, E(K_2, E(K_1, P))$

Note: In the Stallings book, they write $C = E(K_1, D(K_2, E(K_1, P))$, but they also say that one could just as easily do encryption with the second step. Since I think this is more intuitive, I've chosen that to put in our notes.

Due to having three layers, the meet in the middle attack previously presented, which takes O(n) time and O(n) space, where $n = 2^{56}$, no longer works because the output of the first encryption step is not equal to the output of the first decryption step.

Both of these versions were commonly used for many years to provide more security than DES and technically are still secure, since computers can't yet quickly try 2^{112} or 2^{168} possible key combinations.