Triple DES

It has been demonstrated through exhaustive key search attacks that DES can be broken. AES is a new cipher alternative to DES. Prior to AES, multiple encryption approach was used with DES implementations. Triple-DES is the most chosen form.

In Triple-DES, 3 encryptions are done. It can be done with 2 keys with E-D-E sequence. It is evident that encrypt operation & decrypt operation are equivalent in security.

$$C = E_{K1}(D_{K2}(E_{K1}(P)))$$

Although are no practical attacks on two-key Triple-DES, there have been several proposed impractical attacks which might become basis of future attacks. Henceforth, Triple-DES with Three-Keys can be used to avoid these possible attacks.

$$C = E_{K3}(D_{K2}(E_{K1}(P)))$$