Variants of DES:

2-DES /Double DES

3-DES/Triple DES

2-DES:

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

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

Meet-in-the-Middle Attack:

- Assume $C=E_{k2}(E_{k1}(P))$
- Given the plaintext P and ciphertext C
- Encrypt P using all possible keys k1
- Decrypt C using all possible keys k2
  - Check the result with the encrypted plaintext lists
  - If found match, then test the two resulting keys against a new known plaintext and ciphertext pair
  - If it turns correct, accept them as keys

  N is key size

  L no.of blocks

  M is size of each block

  2^{n+1} (Mi+N) bits

3-DES/Triple DES

--Triple-DES with Two-Keys

$$C = E_{K1}[D_{K2}[E_{K1}[P]]]$$

--Triple-DES with Three-Keys

$$C = E_{K3}[E_{K2}[E_{K1}[P]]]$$

S/MIME,PGP