Meet in the middle attack in Double DES, Triple DES with two different keys, and Triple DES with three different keys.

	Ciphertext for key, K:							
P	*000*	*001*	*010*	*011*	*100*	*101*	*110*	*111*
00000	00001	10010	01101	01111	11011	10011	10000	11101
00001	10001	01001	11010	10000	01010	11100	10100	01010
00010	01011	10100	11011	01100	00100	10100	00111	00100
00011	01110	10110	01011	00111	10110	11101	11000	00101
00100	00011	00011	00001	11101	11001	10010	11011	01100
00101	10100	10111	01110	00010	01101	00011	01101	00110
00110	10101	11111	00110	10011	00010	10001	10111	10110
00111	01101	10001	10111	00110	11111	01100	11100	10011
01000	01000	11011	10011	01010	01001	10110	10011	11111
01001	10010	11110	10001	10101	01111	00100	00000	01110
01010	01111	00010	10000	10110	11000	01010	00001	00010
01011	11110	01110	00111	01011	11101	11011	01111	10010
01100	11011	10000	01010	00101	01100	00101	01100	00111
01101	11101	00111	10110	01000	01000	10111	10010	11100
01110	11000	01000	10100	00000	11010	01111	11111	01000
01111	01001	11101	01100	00001	00011	01000	01010	01101
10000	00110	11100	01111	01001	01011	11111	00010	11011
10001	11111	01100	10010	10010	00000	11010	11110	00000
10010	10110	10011	11110	01101	10111	01101	10001	10000
10011	00010	00001	11000	11100	10100	00111	00011	10111
10100	10111	01101	11001	11111	10011	00000	00100	00011
10101	01010	01111	00101	00011	00001	01001	10101	01011
10110	00000	00110	10101	11010	00110	01011	01000	11001
10111	00111	11000	01001	11110	10000	00010	01110	10100
11000	00101	01011	00010	10001	11100	10000	11010	10001
11001	11100	00000	11101	10111	10001	01110	00101	11000
11010	11010	11001	01000	01110	01110	11110	01011	01001
11011	01100	11010	11111	11001	10101	00001	10110	00001
11100	11001	01010	00100	00100	00101	11001	00110	10101
11101	10011	10101	00011	10100	00111	00110	11001	01111
11110	00100	00101	11100	11000	10010	11000	11101	11110
11111	10000	00100	00000	11011	11110	10101	01001	11010

Fig 1

Figure 1 shows an example 5-bit block cipher. Each entry/block cipher is related to one specific plaint text and key.

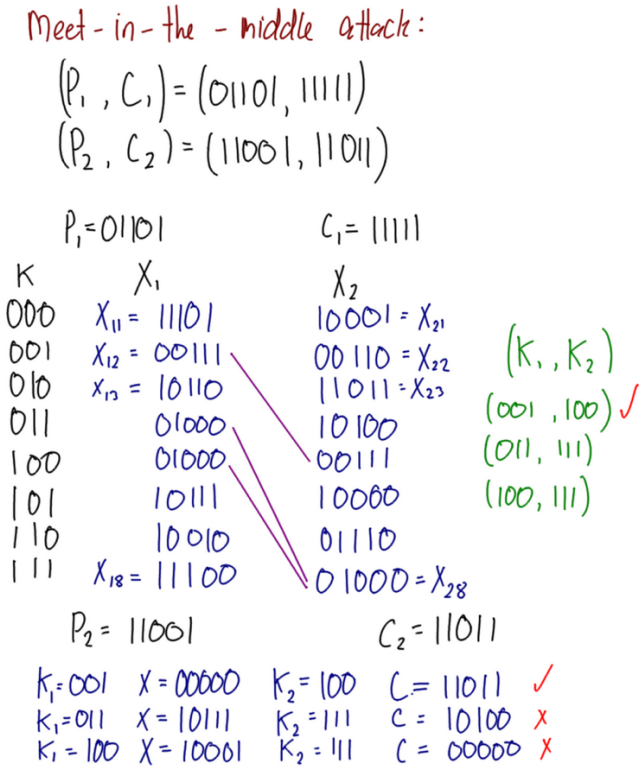
Section 1: Double DES where two keys are K1, K2, C denotes Cipher text, P denotes Plain text, D is the encryption and D is decryption algorithm.

Double Encryption where key K is k-bits: C = E(K2,E(K1,P))
Say X = E(K1,P) = D(K2,C)
Attacker knows two plaintext, ciphertext pairs (Pa,Ca) and (Pb,Cb)

1. Encrypt Pa using all 2k values of K1 to get multiple values of X
2. Store results in table and sort by X
3. Decrypt Ca using all 2k values of K2
4. As each decryption result produced, check against table
5. If match, check current K1,K2 on Cb. If Pb obtained, then accept the keys

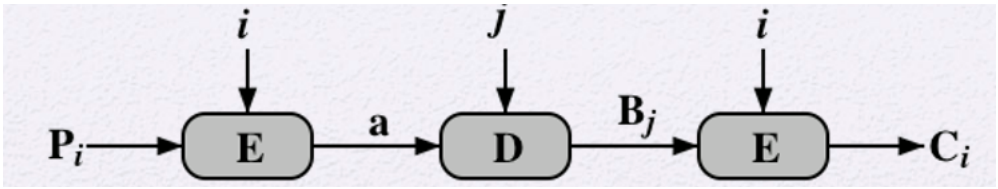
With two known plaintext, ciphertext pairs, probability of successful attack is almost 1
Encrypt/decrypt operations required: $\approx 2 \times 2k$ (twice as many as single encryption)

Examples:
You have obtained the plaintext/ciphertext pairs of two of those messages: (P1,C1) = (01101, 11111) and (P2,C2) = (11001, 11011). Using a meet-in-the-middle attack, find the secret key.



Video: https://www.youtube.com/watch?v=vROZGQ9XLe8

Section 2: Triple DES with two different keys, i.e., C=E(i, D(j, E(i,P))), where i represents the first key and j is the second key.



The best attack to 3DES is due to van Oorschot and Wiener and goes as follows.

1. Guess the first intermediate value, a

2. for each possible value of i, list possible values of the second intermediate value, b.
   The step will contain multiple small steps:
   (1) get corresponding plain text for the fixed a and every possible i, i.e., P_i'=D(i, a), for all i;

(2) check if the prior knowledge (known plaintext-ciphertext pairs) has the plain text derived from step (1)
(3) if answer is yes. Assume we have a pair of known plaintext-ciphertext which is (P, C) where P equals to P_i' from step (1). Then we get the possible value b as D(i, C) where C is from the pair of known plaintext-ciphertext and i is the key.
(4) If answer is no. Go to Step 1.

3. For each possible j, elements with a matching second intermediate value, b: b=E(j, a)

4. Check if possible values of B from step 2 matches possible values of B from step 3. If there is a match, then the corresponding i, j are the first and second key. The probability of a match is $\frac{k}{2^{64}}$, where k is the number of pair of known plaintext-ciphertext.

The whole attack requires $\frac{2^{64+56}}{k}$ time and k storage.

Examples:
You have obtained the plaintext/ciphertext pairs of two of those messages: (P_a,C_a) = (01101, 01110) and (P_b,C_b) = (11001, 00100). Using a meet-in-the-middle attack, find the secret key.

1. Guess the first intermediate value a, where a is randomly picked. Assume a=00111.
2. For each possible i, get possible values of B
(1)

a=00111	Key i	$P_i' = D(i, a)$
	000	10111
	001	01101
	010	01011
	011	00011
	100	11101
	101	10011
	110	00010
	111	01100

(2) and (3): $P_a = 01101$ equals to P'_{001}, so the possible values of B is D(001, C_a)=D(001, 01110)=01011

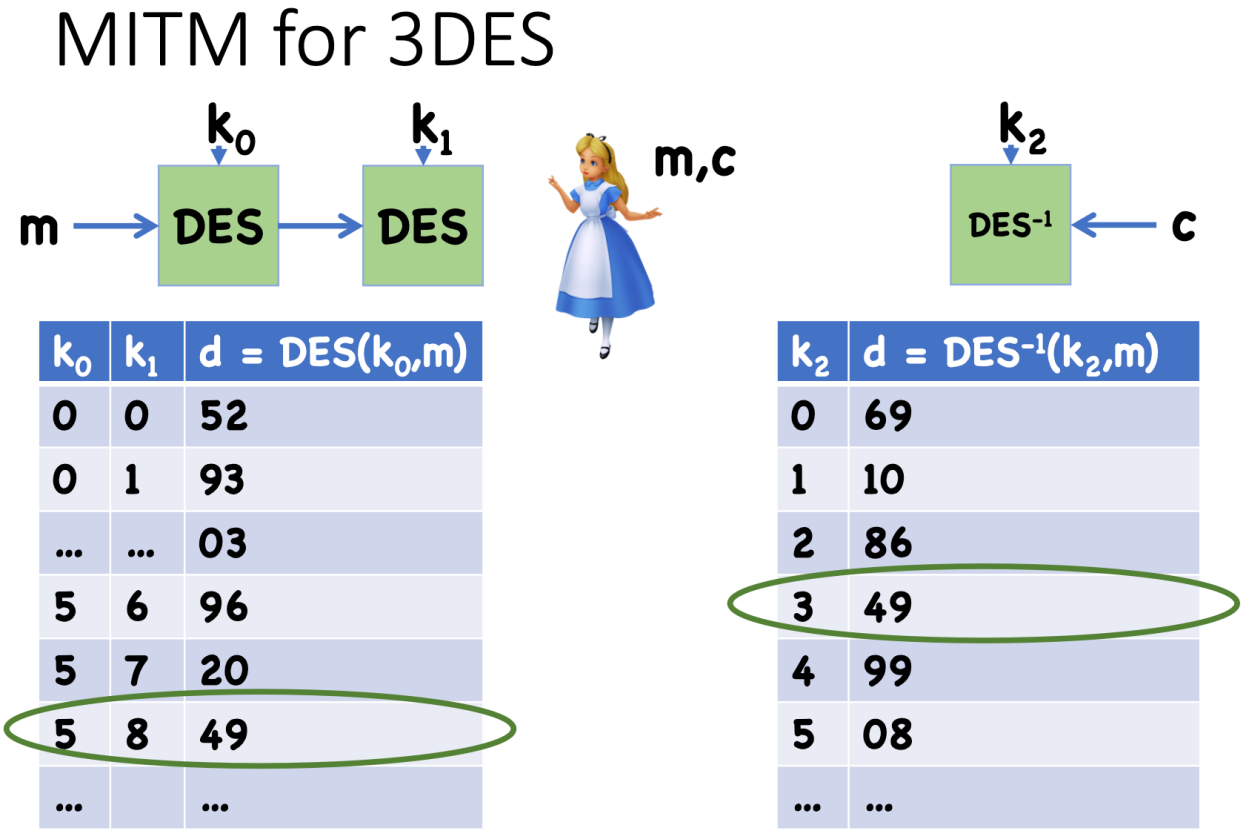
3. For each possible j, get possible values of B, e.g., D(j, a)

a=00111	Key i	$D(j, a)$
	000	10111
	001	01101
	010	01011
	011	00011
	100	11101

	101	10011
	110	00010
	111	01100

4. Match. We find j=010, D(j, a)=01011 matches B's value from step 2. So (i, j)=(001.010).

Triple DES with three different keys.



1: try every possible combination of k0 and k1. As key size is 56 bits in DES, so there are 2^{112} possible combinations of k0 and k1. We can get the potential intermediate values after 2 times encryption.

2: try every possible case of k3. There are 2^{56} possible values of k3. We can get the potential intermediate values after one decryption

3: compare two tables to find if there is a match.

While 3DES with three different keys has 168 bit keys, effective security is 112 bits