Multiple Encryption

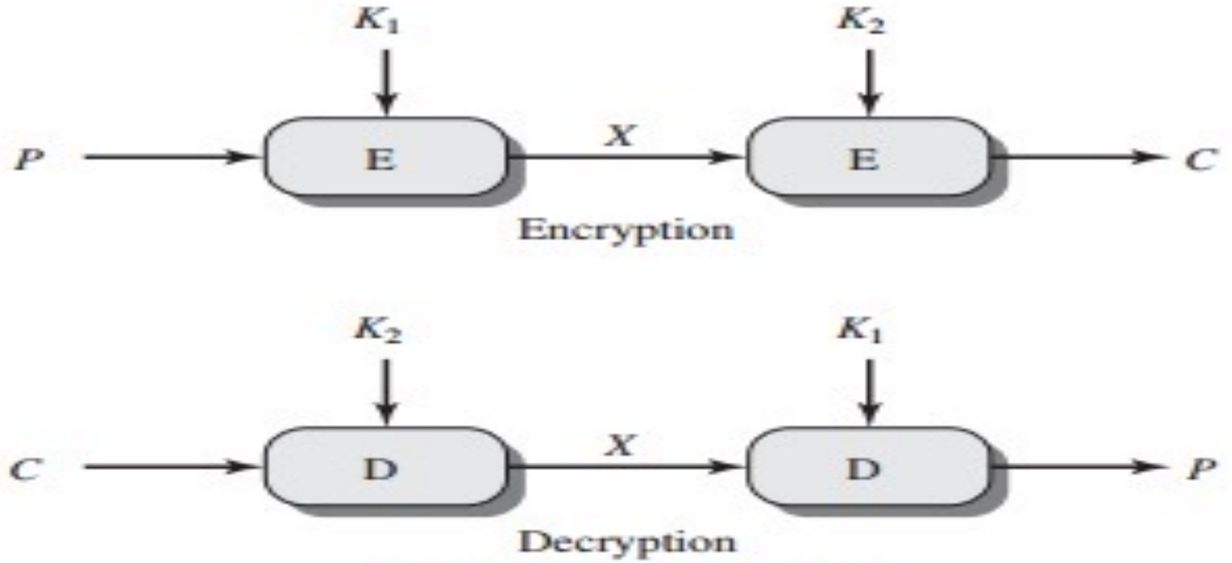
Multiple encryption is a technique in which an encryption algorithm is used multiple times.

Double DES

- The simplest form of multiple encryption has **two encryption stages and two keys** Given a plaintext P and two encryption keys $K1$ and $K2$, ciphertext C is generated as
  - $C = \mathrm{E}(K2, \mathrm{E}(K1, P))$
- Decryption requires that the keys be applied in reverse order:
  - $P = \mathrm{D}(K1, \mathrm{D}(K2, C))$
- For DES, this scheme apparently involves a key length of 56 * 2 = 112 bits, resulting in a dramatic increase in cryptographic strength.

$$C = \mathrm{E}(K2, \mathrm{E}(K1, P))$$

$$P = \mathrm{D}(K1, \mathrm{D}(K2, C))$$

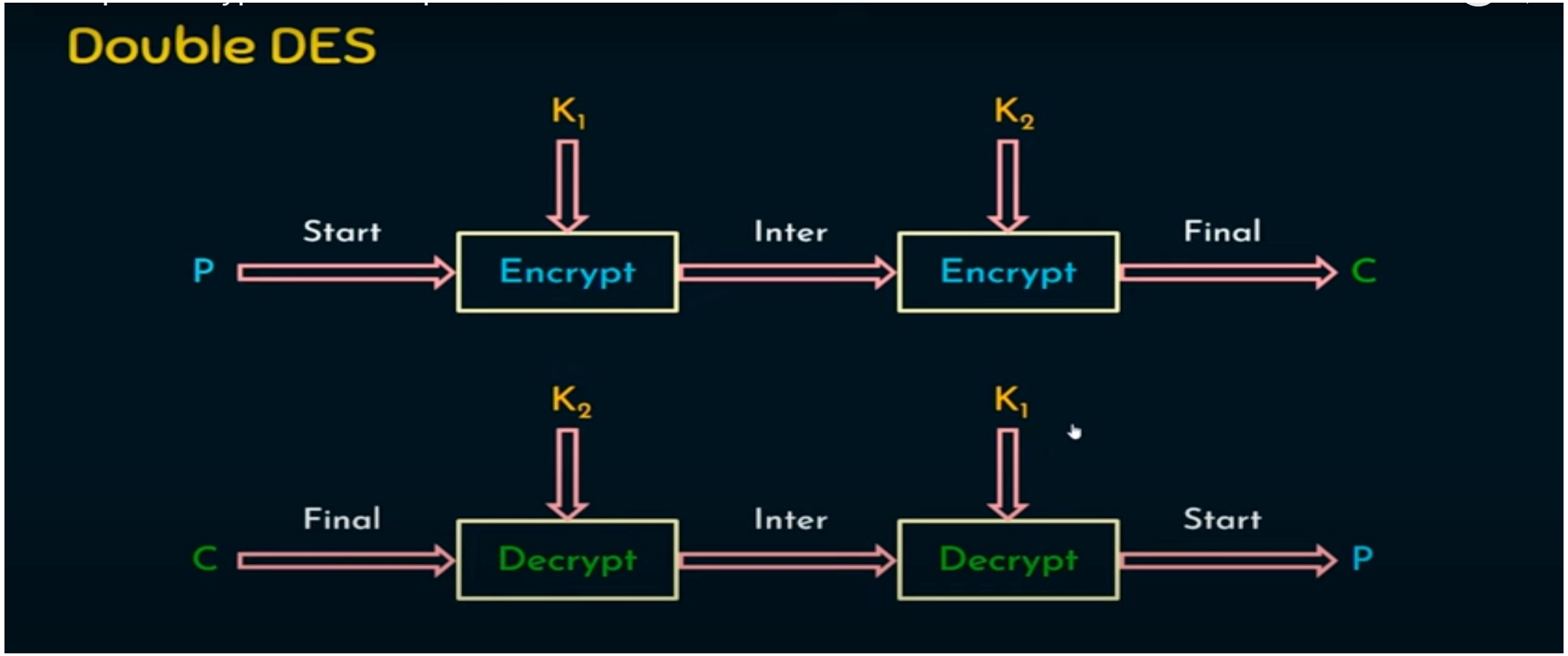


(a) Double encryption

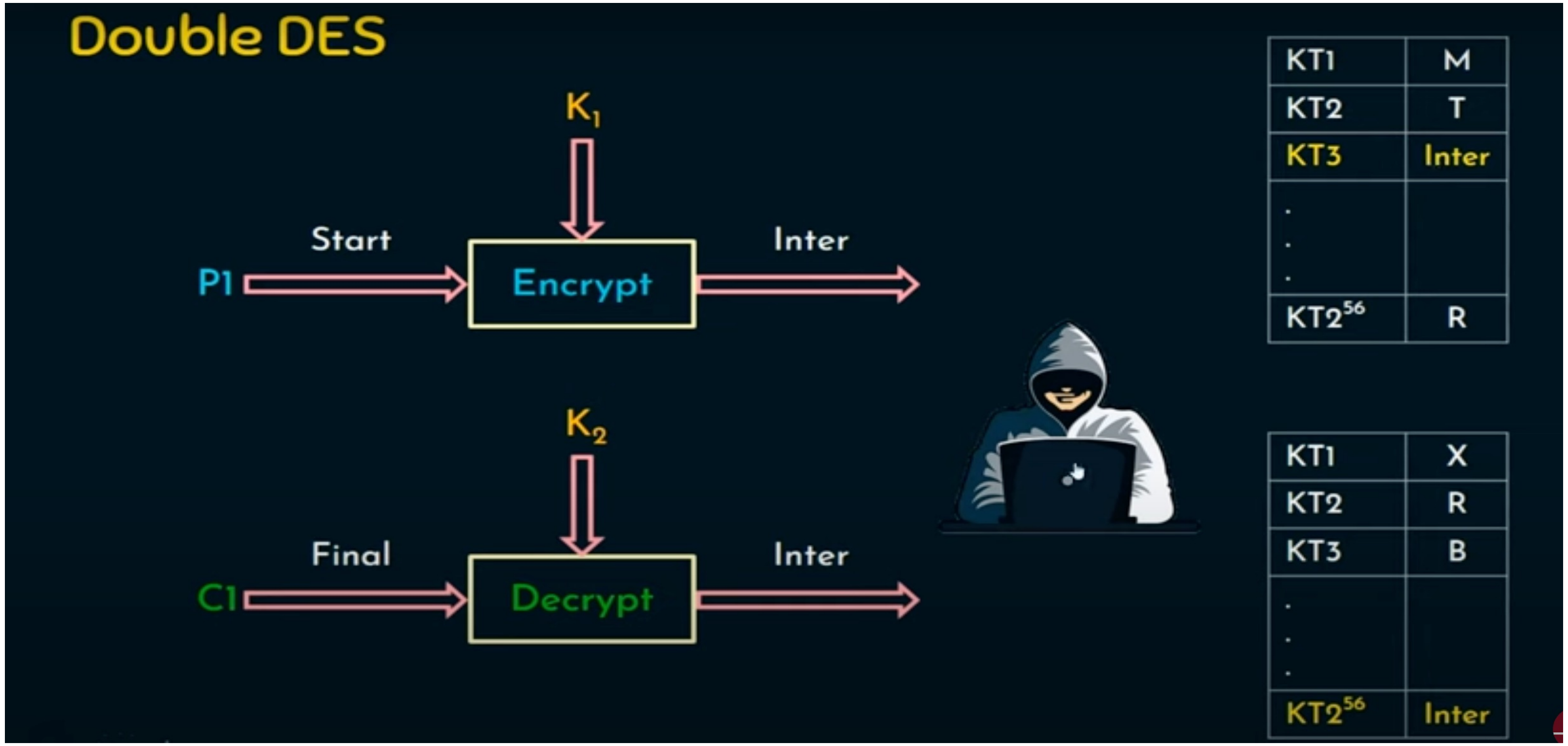
Meet in the Middle Attack

- Given a known pair, (*P*, *C*), the attack proceeds as follows.
- First, encrypt *P* for all 2^{56} possible values of *K*1.
- Store these results in a table
- Next, decrypt *C* using all 2^{56} possible values of *K*2.
- As each decryption isproduced, check the result against the table for a match.
- If a match occurs, then test the two resulting keys against a new known plaintext–ciphertext pair.

Plain Text:Start
Cipher Text: Final



Double DES

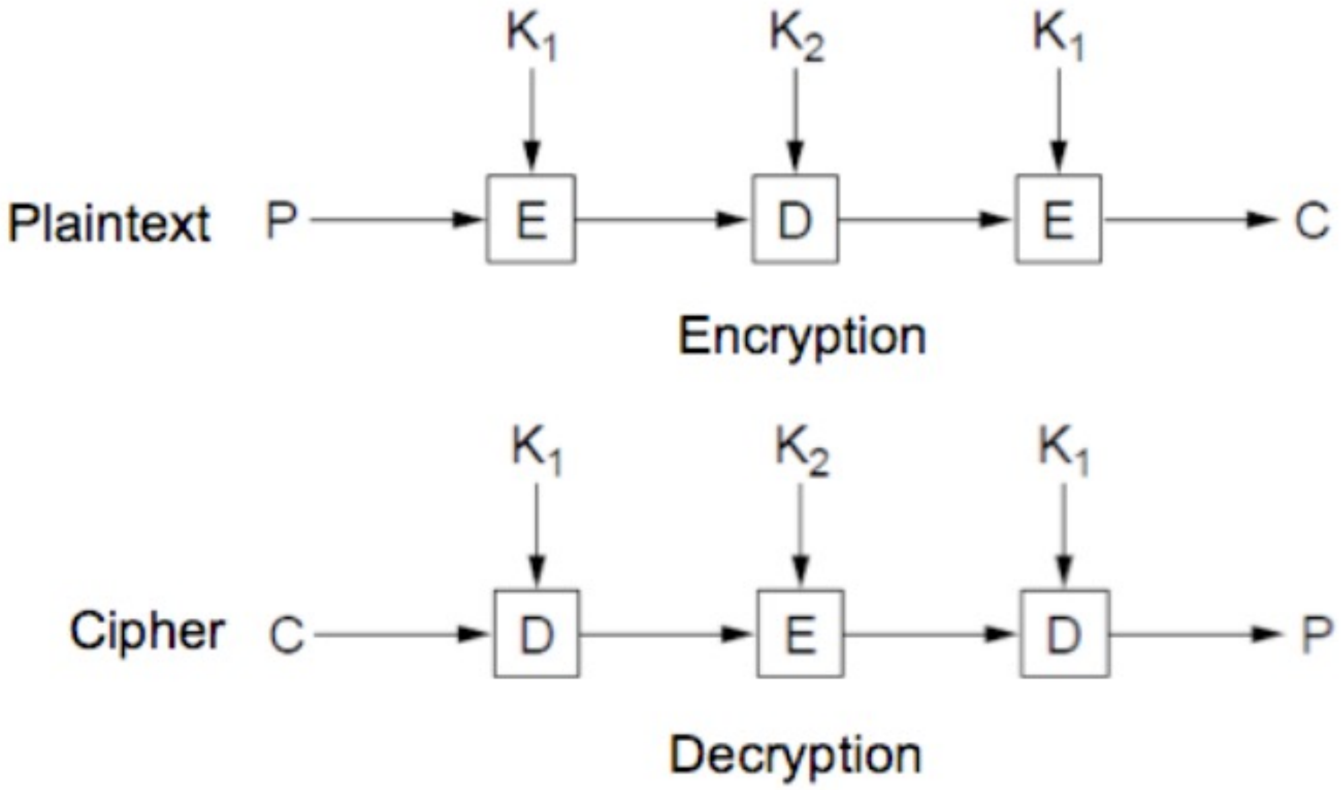


Double DES

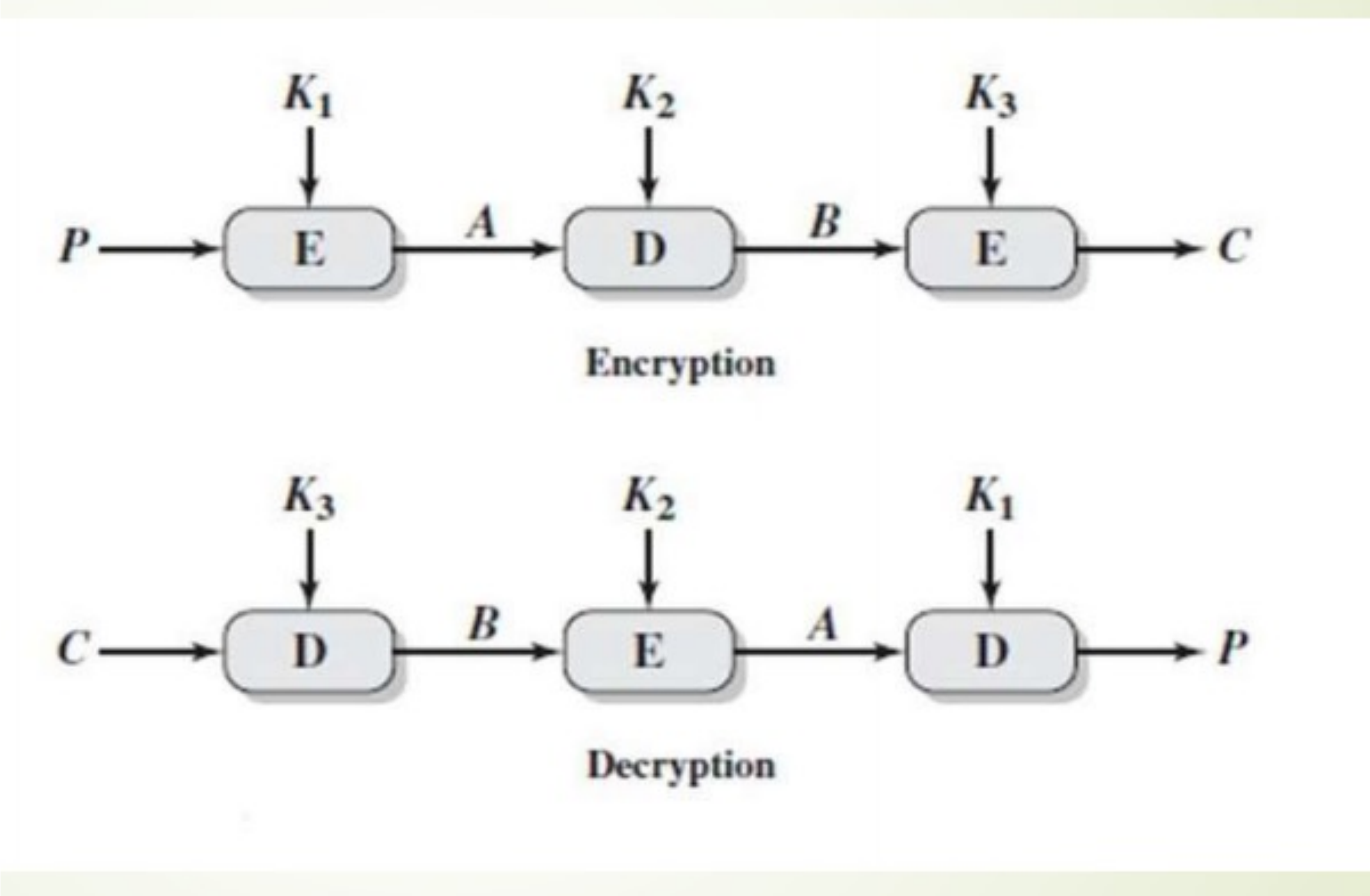
KT1	M
KT2	T
KT3	Inter
. . .	
KT2^{56}	R

KT1	X
KT2	R
KT3	B
. . .	
KT2^{56}	Inter

Triple DES with 2 Keys



Triple DES with 3 Keys



K_1
K_2
K_3
P
E
A
D
B
E
C
Encryption
K_3
K_2
K_1
C
D
B
E
A
D
P
Decryption