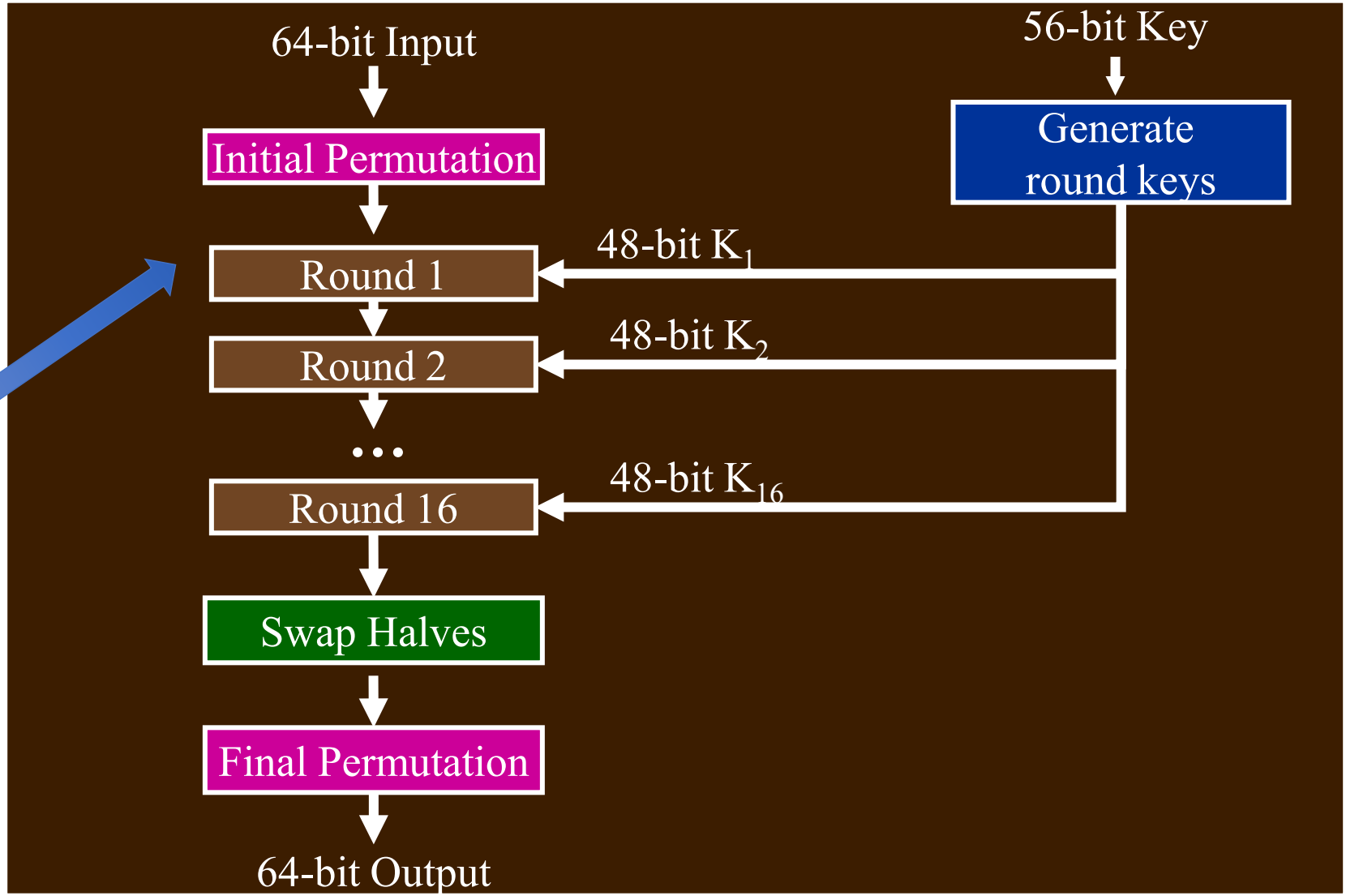
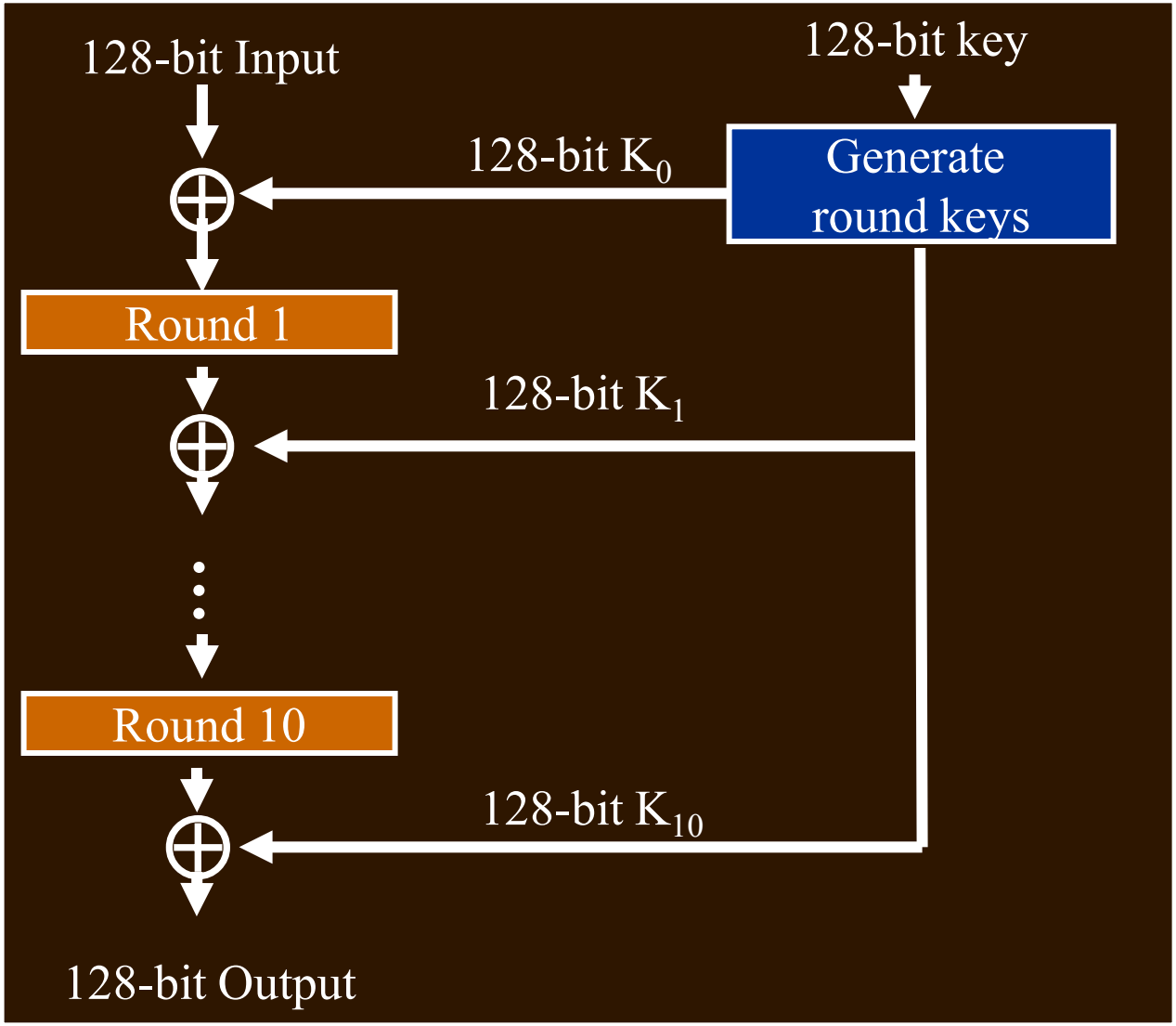
CS 4173/5173
COMPUTER SECURITY

Modes of Operation

OUTLINE LAST TIME: DES

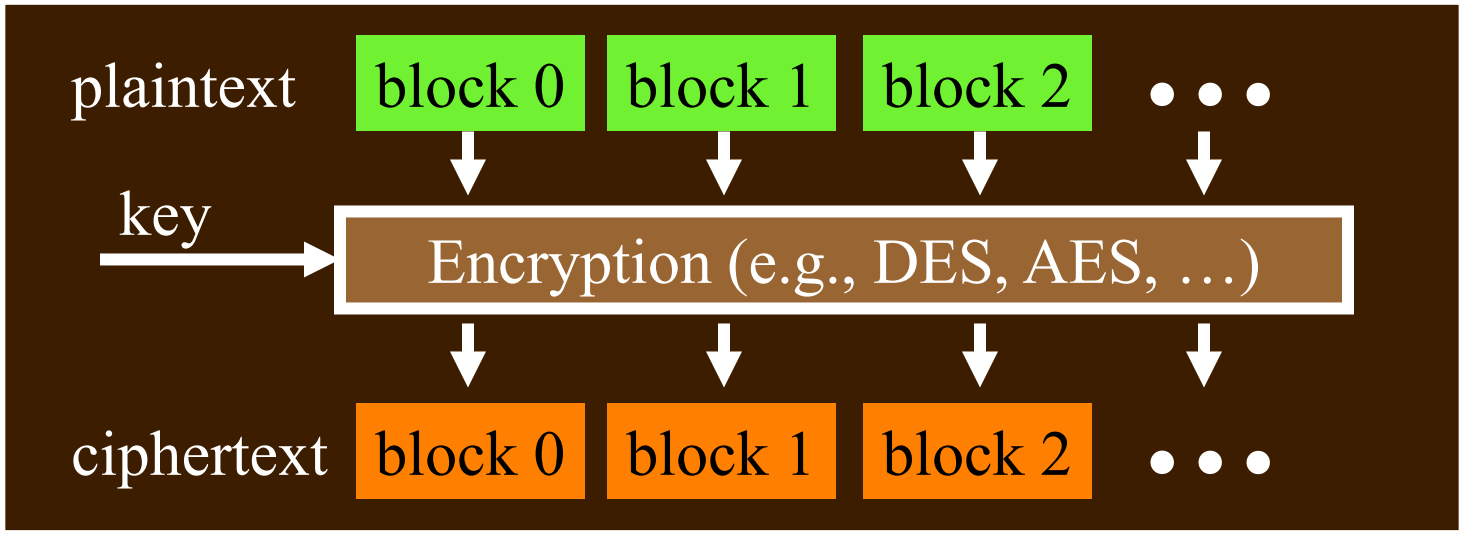


OUTLINE LAST TIME: AES



A REMAINING ISSUE FOR BLOCK CIPHER

- How block cipher works



- Question: How to transmit the ciphertext blocks ?

PROCESSING WITH BLOCK CIPHERS

- Most ciphers work on blocks of fixed (small) size
- How to chain cipher text together?
- Modes of operation: describe how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)
  - CFB (Cipher Feedback)
  - CTR (Counter)

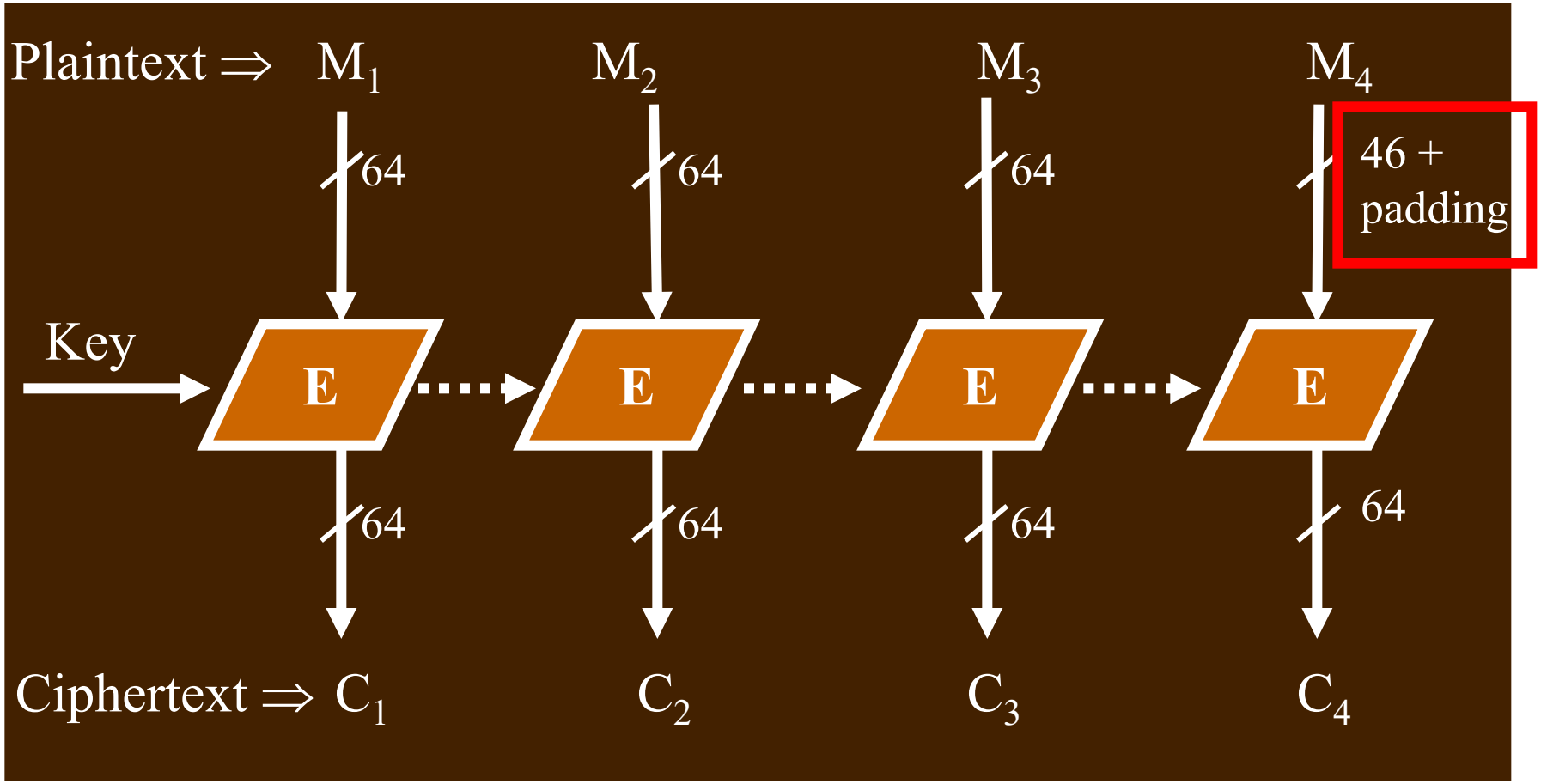
ISSUES FOR BLOCK CHAINING MODE

- Information leakage
  - Does it reveal info about the plaintext blocks?
    - E.g., two cipher blocks have the same information?
- Ciphertext manipulation
  - Can an attacker modify ciphertext block(s) in a way that will produce a predictable/desired change in the decrypted plaintext block(s)?
  - Note: assume the structure of the plaintext is known, e.g., first block is employee #1 salary, second block is employee #2 salary, etc.

ISSUES… (CONT'D)

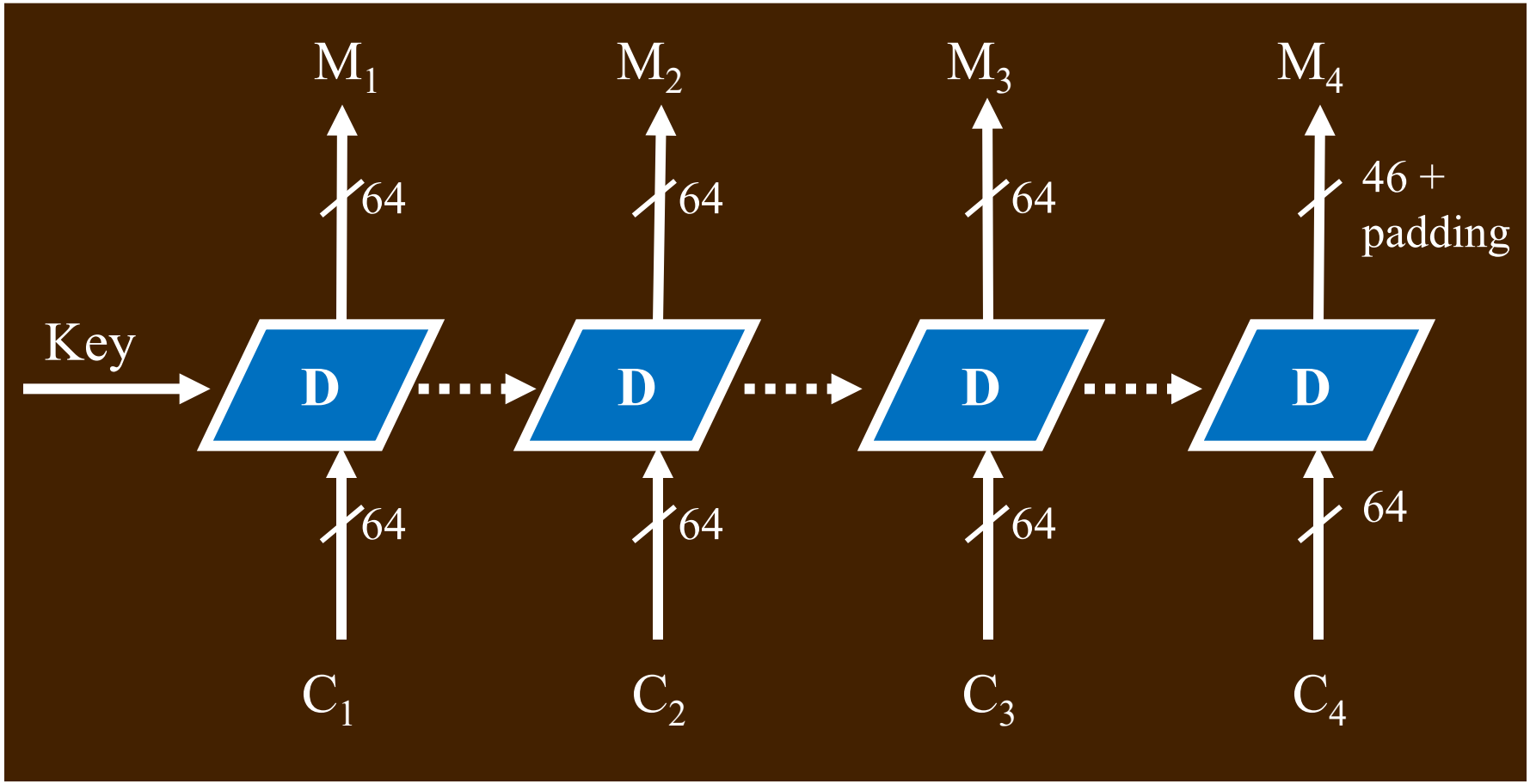
- Parallel/Sequential
  - Can blocks of plaintext (ciphertext) be encrypted (decrypted) in parallel?
- Error propagation
  - If there is an error in a plaintext (ciphertext) block, will there be an encryption (decryption) error in more than one ciphertext (plaintext) block?

ELECTRONIC CODE BOOK (ECB)



- The easiest mode of operation; each block is independently encrypted

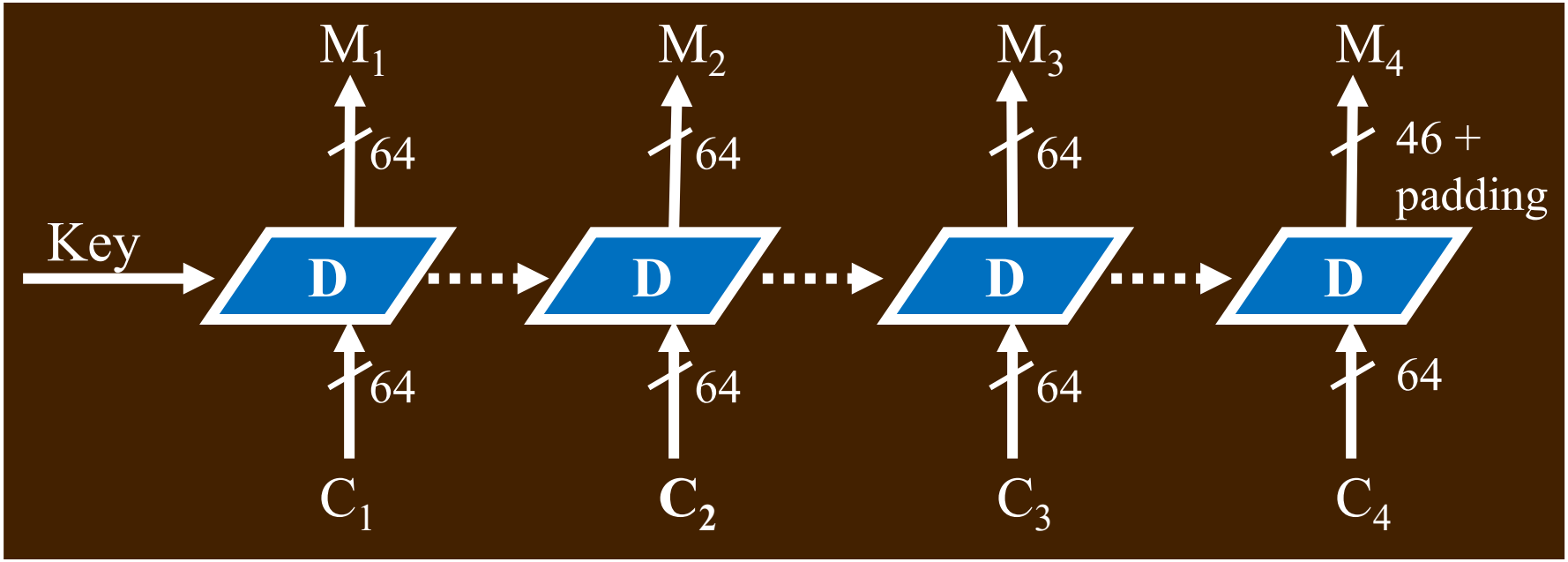
ECB DECRYPTION



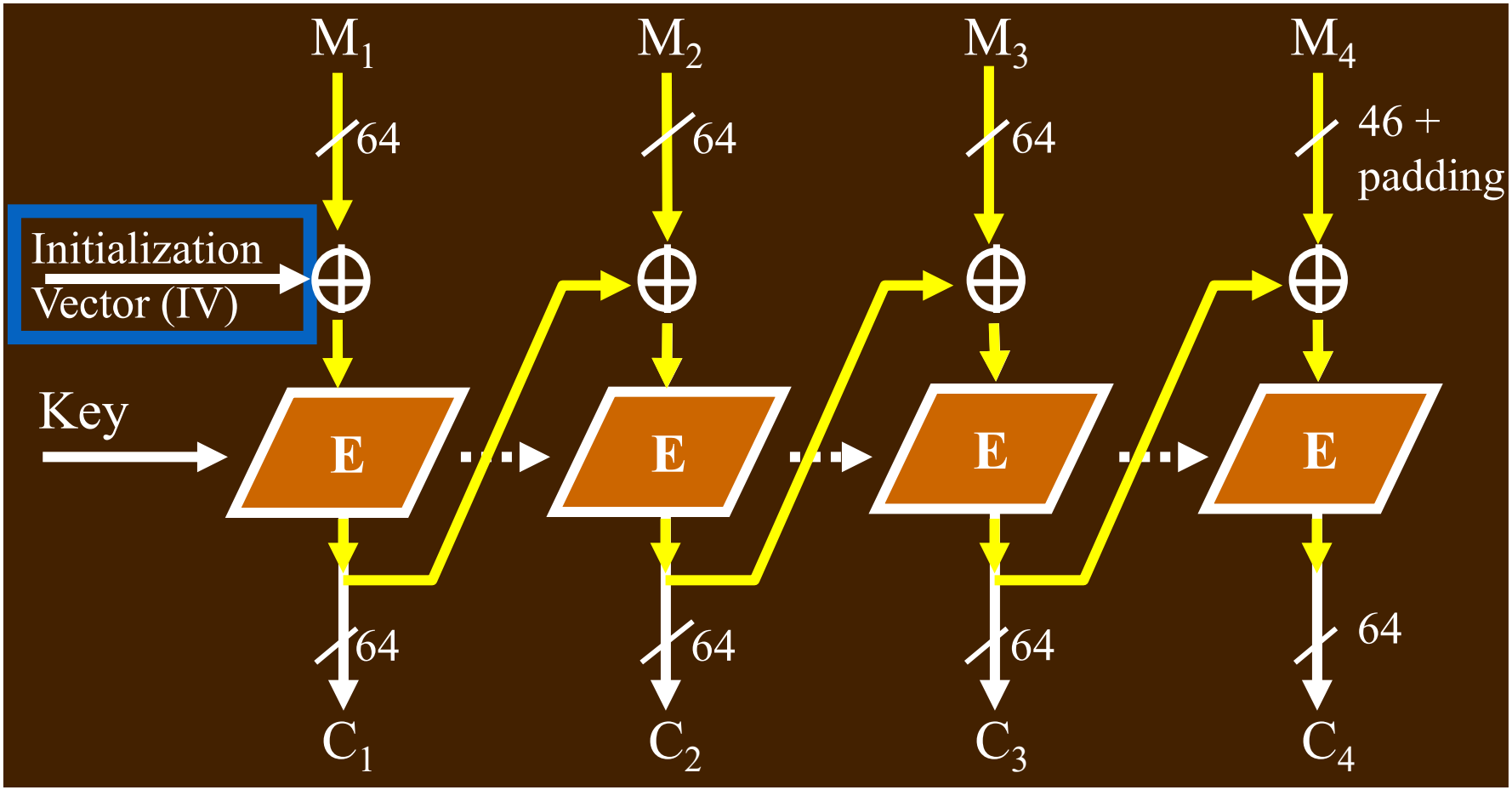
- Each block is independently decrypted

ECB PROPERTIES

- Does information leak? Yes
- Can ciphertext be manipulated? Yes
- Parallel processing possible? Yes
- Do ciphertext errors propagate? no



CIPHER BLOCK CHAINING (CBC)

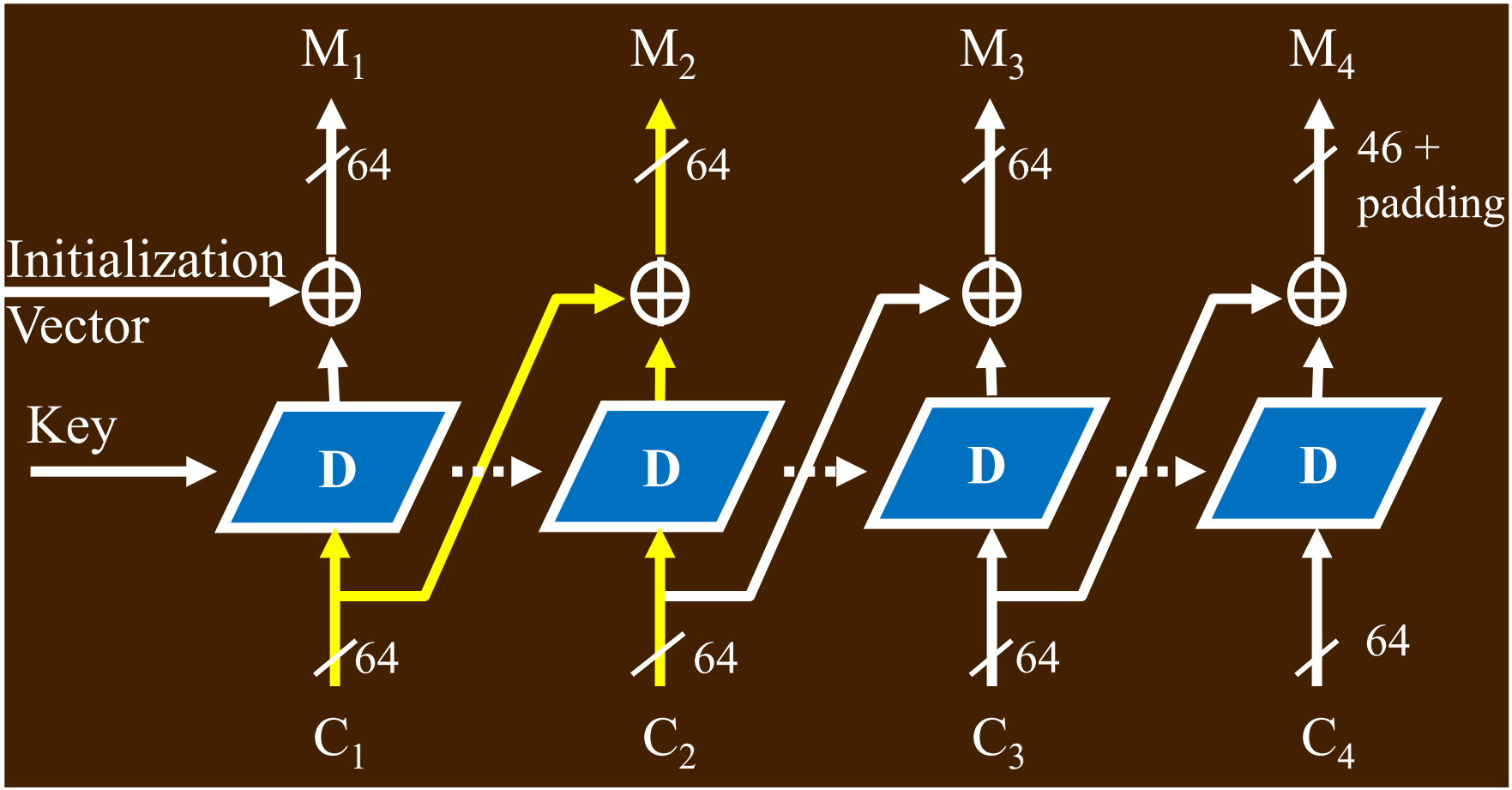


- Chaining dependency: each ciphertext block depends on all preceding plaintext blocks

INITIALIZATION VECTORS

- Initialization Vector (IV)
  - Used along with the key; not secret
  - For a given plaintext, changing either the key, or the IV, will produce a different ciphertext
  - Why is that useful?
- IV generation and sharing
  - Random; may transmit with the ciphertext
  - Incremental; predictable by receivers

CBC DECRYPTION

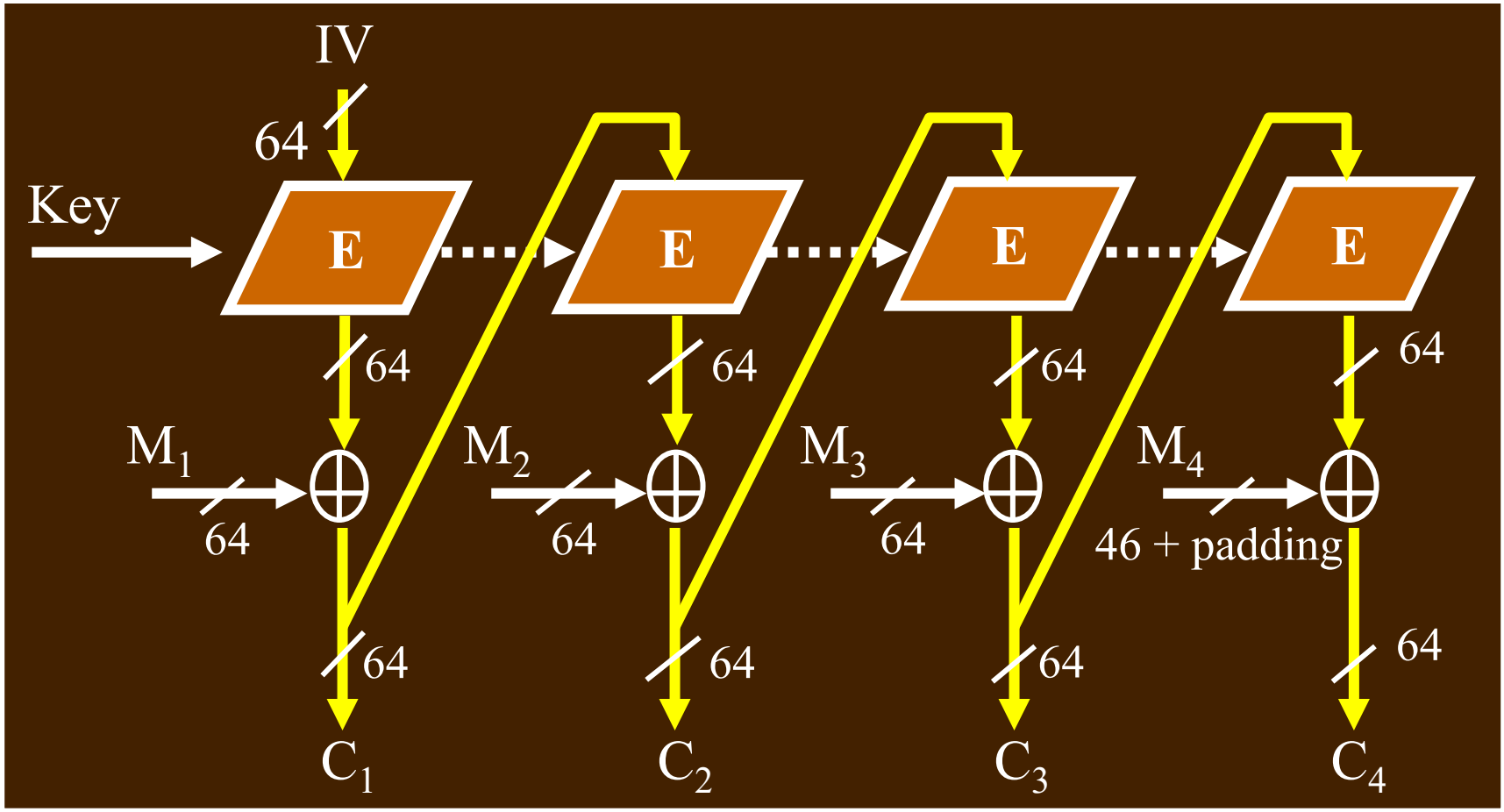


- How many ciphertext blocks does each plaintext block depend on?

CBC PROPERTIES

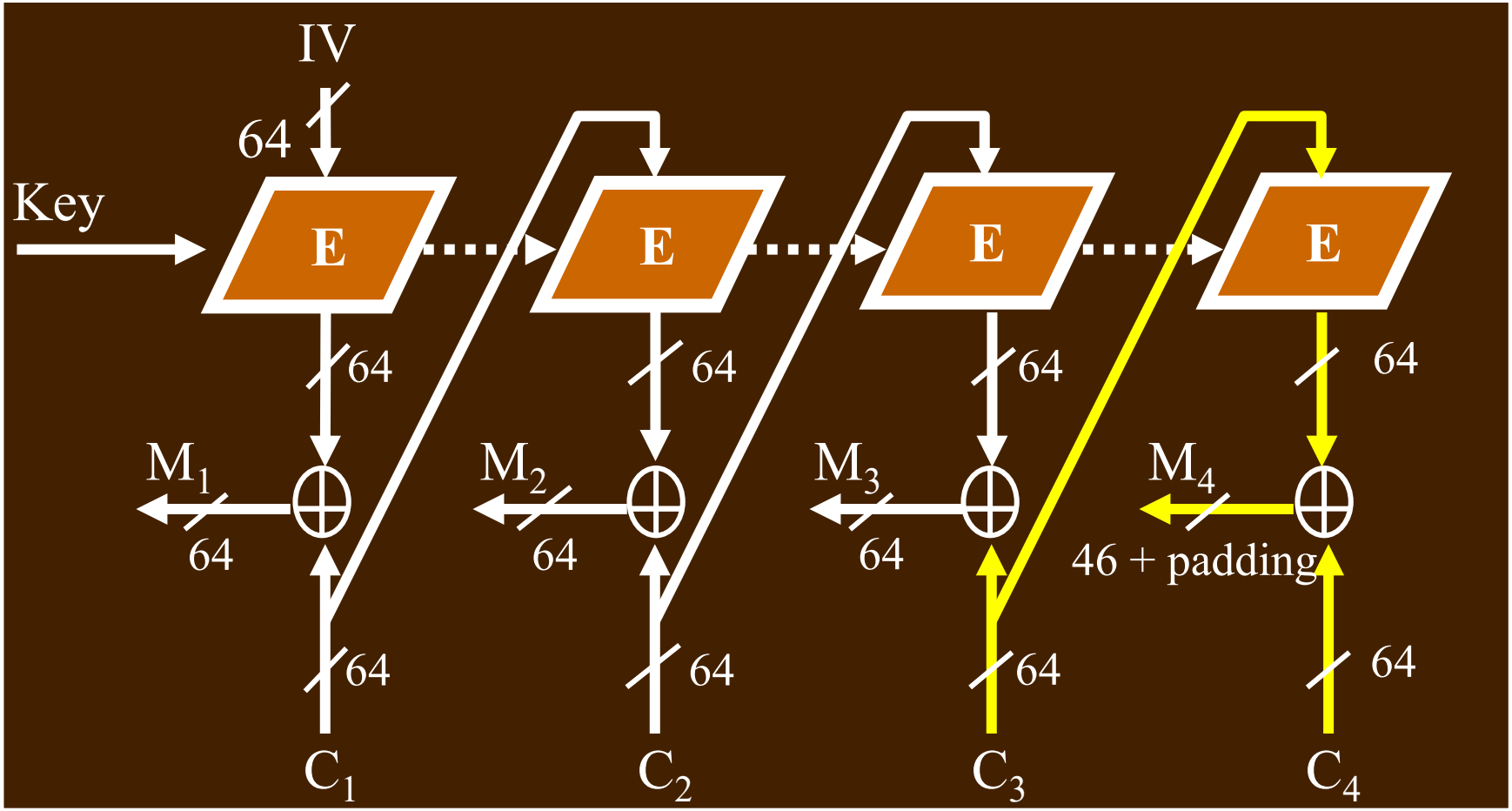
- Does information leak?
  - Identical plaintext blocks will produce different ciphertext blocks
- Can ciphertext be manipulated?
  - Yes, but no easy swap
- Parallel processing possible?
  - no (encryption), yes (decryption)
- Do ciphertext errors propagate?
  - Yes for encryption, no for decryption.

CIPHER FEEDBACK MODE (CFB)



- Ciphertext block C_j depends on all preceding plaintext blocks

CFB DECRYPTION

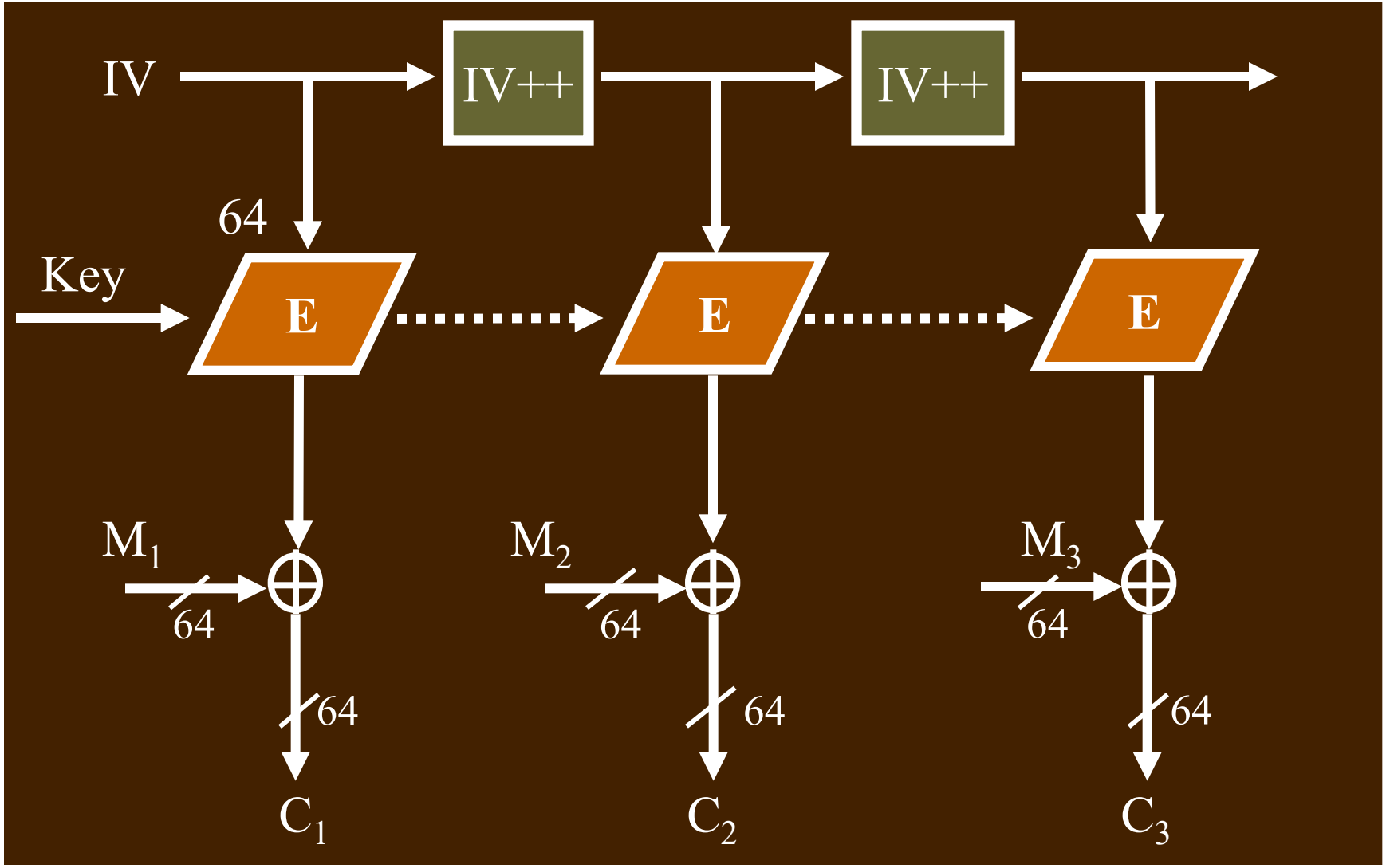


- No block decryption required!

CFB PROPERTIES

- Does information leak?
  - Identical plaintext blocks produce different ciphertext blocks
- Can ciphertext be manipulated?
  - Yes, but no easy swap
- Parallel processing possible?
  - no (encryption), yes (decryption)
- Do ciphertext errors propagate?
  - yes(encryption), no (decryption)

COUNTER MODE (CTR)



CTR MODE PROPERTIES

- Does information leak?
  - Identical plaintext block produce different ciphertext blocks
- Can ciphertext be manipulated?
  - Yes, but no easy swap
- Parallel processing possible
  - Yes
- Do ciphertext errors propagate?
  - No

CS 4173/5173
COMPUTER SECURITY

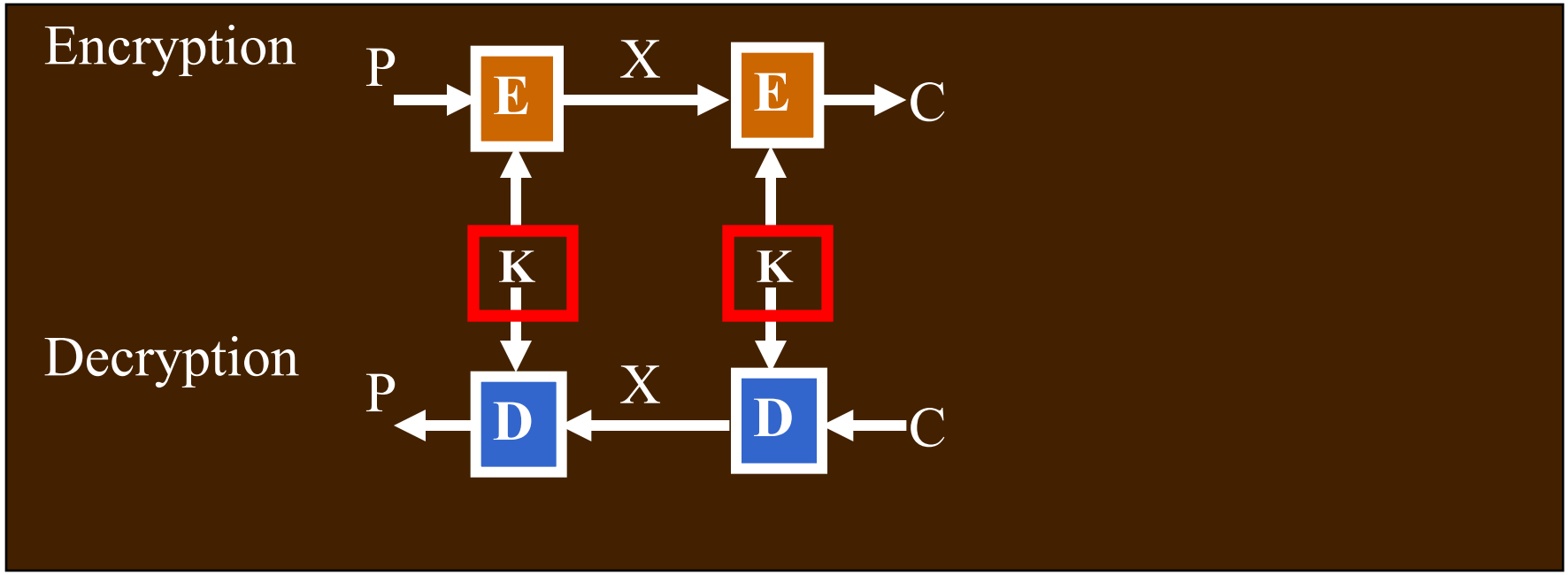
Triple DES

STRONGER DES

- Major limitation of DES
  - Key length is too short
- Can we apply DES multiple times to increase the strength of encryption?

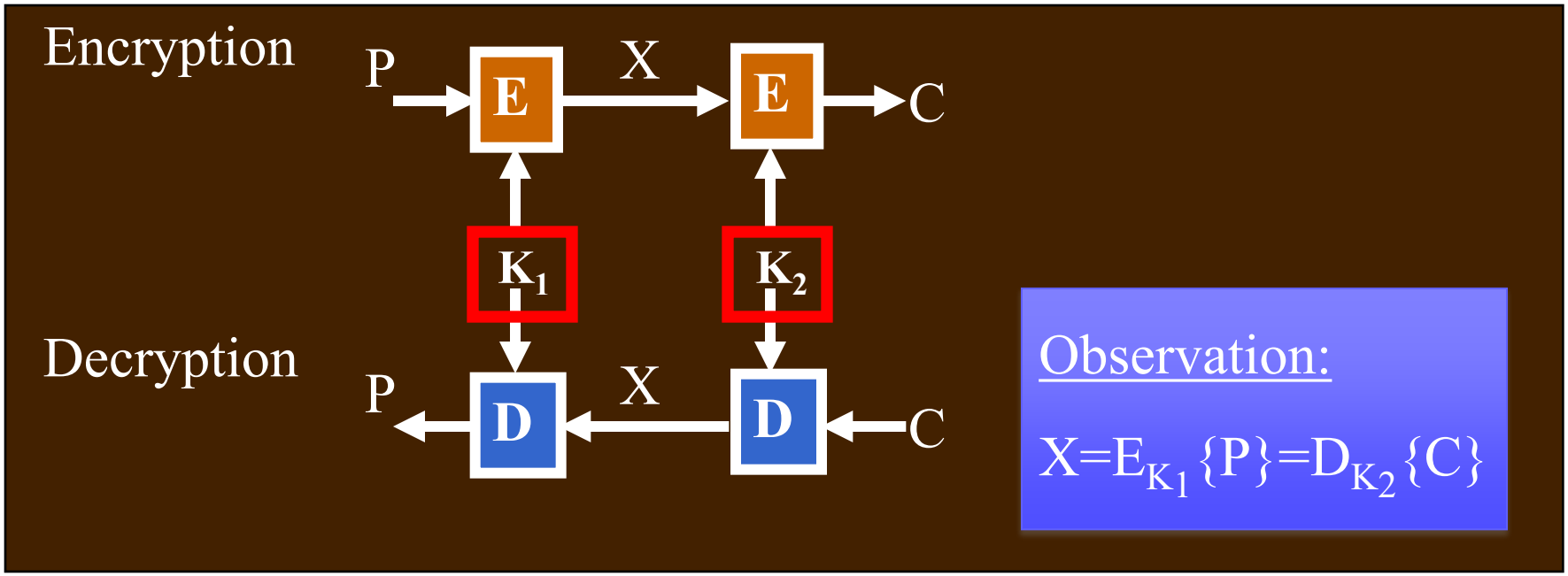
DOUBLE ENCRYPTION WITH DES

- Does encrypting using the same key make things more secure?



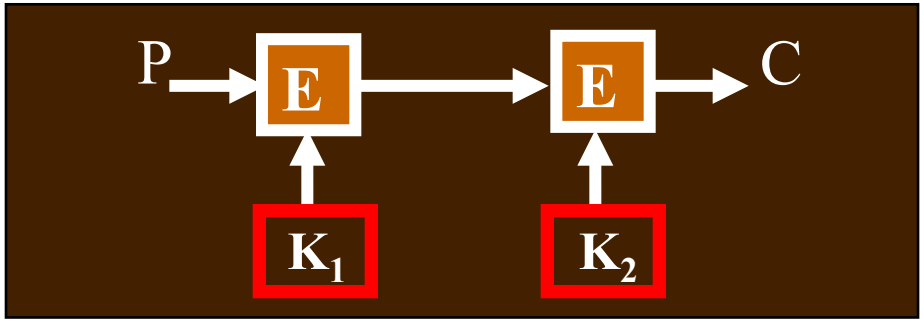
DOUBLE ENCRYPTION WITH DES

- Encrypt the plaintext twice, using two different DES keys
- Total key material increases to 112 bits
  - is that the same as key strength of 112 bits?



THE MEET-IN-THE-MIDDLE ATTACK

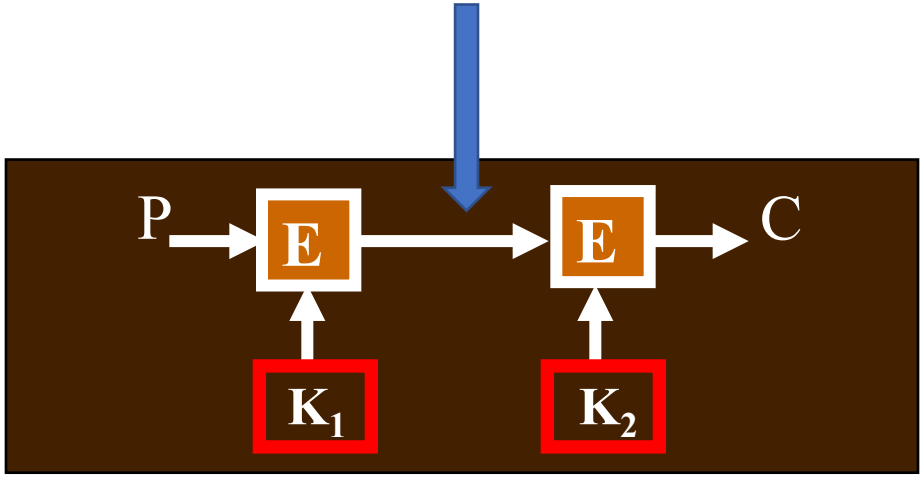
- Procedure: http://en.wikipedia.org/wiki/Meet-in-the-middle_attack
- An Attack Example
  - Double DES with two different keys K_1 and K_2
    - Total key size: 56 + 56 = 112 bits.
    - The cost of exhaustive search? -> 100 quadrillion years
    - What is the cost to crack DES (56 bits) ? -> 700 seconds
  - The attacker knows a plaintext P and ciphertext C.



ATTACKER'S OBSERVATION

Some intermediate text **I**

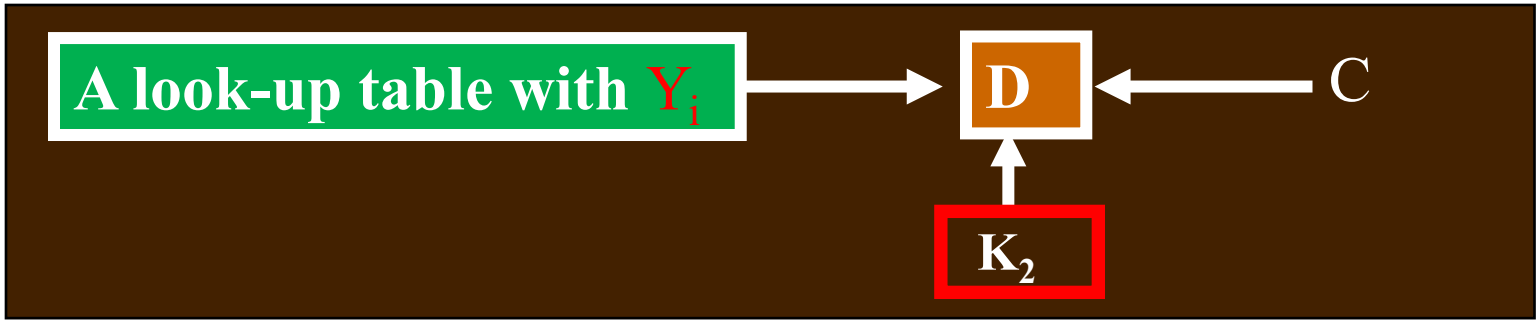
K_1(P)=I, K_2(I)=C



ATTACK PROCEDURE

1. encrypt P using single-DES for all possible 2^{56} values K_1 to generate all possible single-DES ciphertexts for P: $X_1, X_2, \ldots, X_{2^{56}}$; The table contains the intermediate text I.

2. decrypt C using single-DES for all possible 2^{56} values K_2 to generate all possible single-DES plaintexts for C: $Y_1, Y_2, \ldots, Y_{2^{56}}$; The table also contains I.



ATTACK PROCEDURE … (CONT'D)

- On Average: the expected number of pairs that result in identical X and Y is 2^{48}.
  - Each (X, Y) pair corresponds to different key pair (K1, K2).
  - Then the attack just needs to try all the pairs.

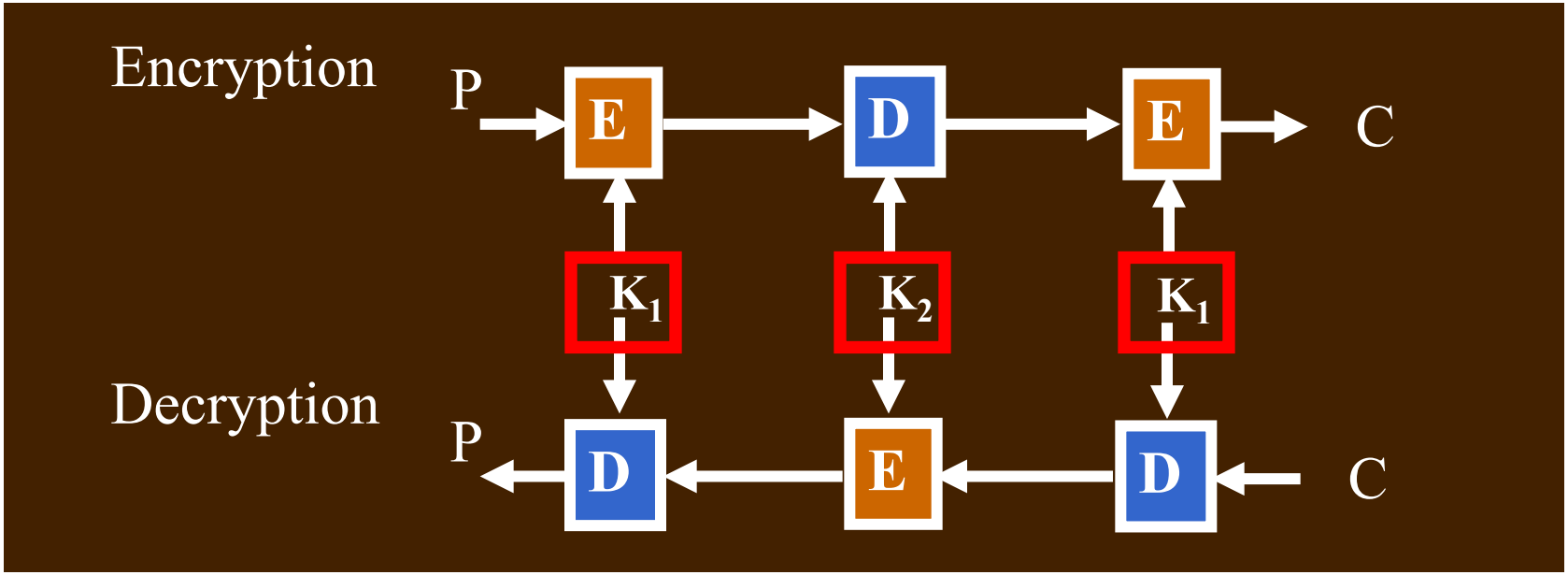
- Total computational cost:
  - $2\times 2^{56} + 2\times 2^{48} < 2^{58}$(vs exhaustive search 2^{112})
- Also huge storage cost.
  - 2^{56} bytes = 65536 TB = 65.5 PB (quite possible for today)
    - Internet materials: "In 2013, Randall Munroe compiled published assertions about Google's data centers, and estimated that the company has about 10 exabytes (10,000 PB) stored on disk… The company has refused to comment on Munroe's estimate."
    - Around $35,000 per PB. --- in 2019

CONCLUSION

- Double DES is not totally secure!

- Meet-in-the-Middle Attack is a generic attack against double-encryption.

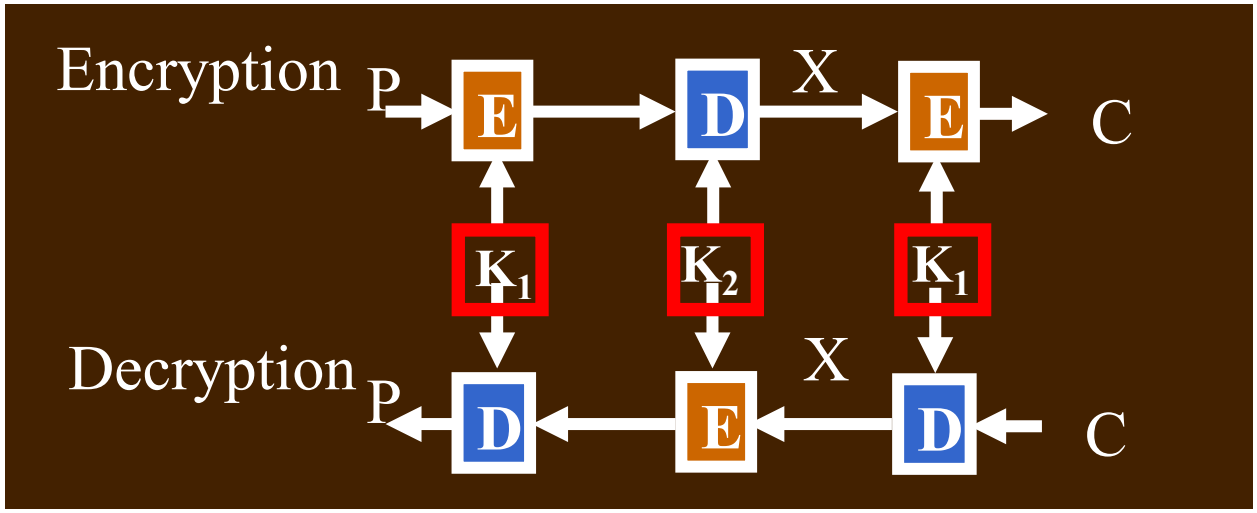
TRIPLE ENCRYPTION (TRIPLE DES-EDE)



- Apply DES encryption/decryption three times

TRIPLE DES (CONT'D)

- Strength:
  - equivalent strength to using a 112 bit key
  - resilient to M-I-T-M attack



Observation:

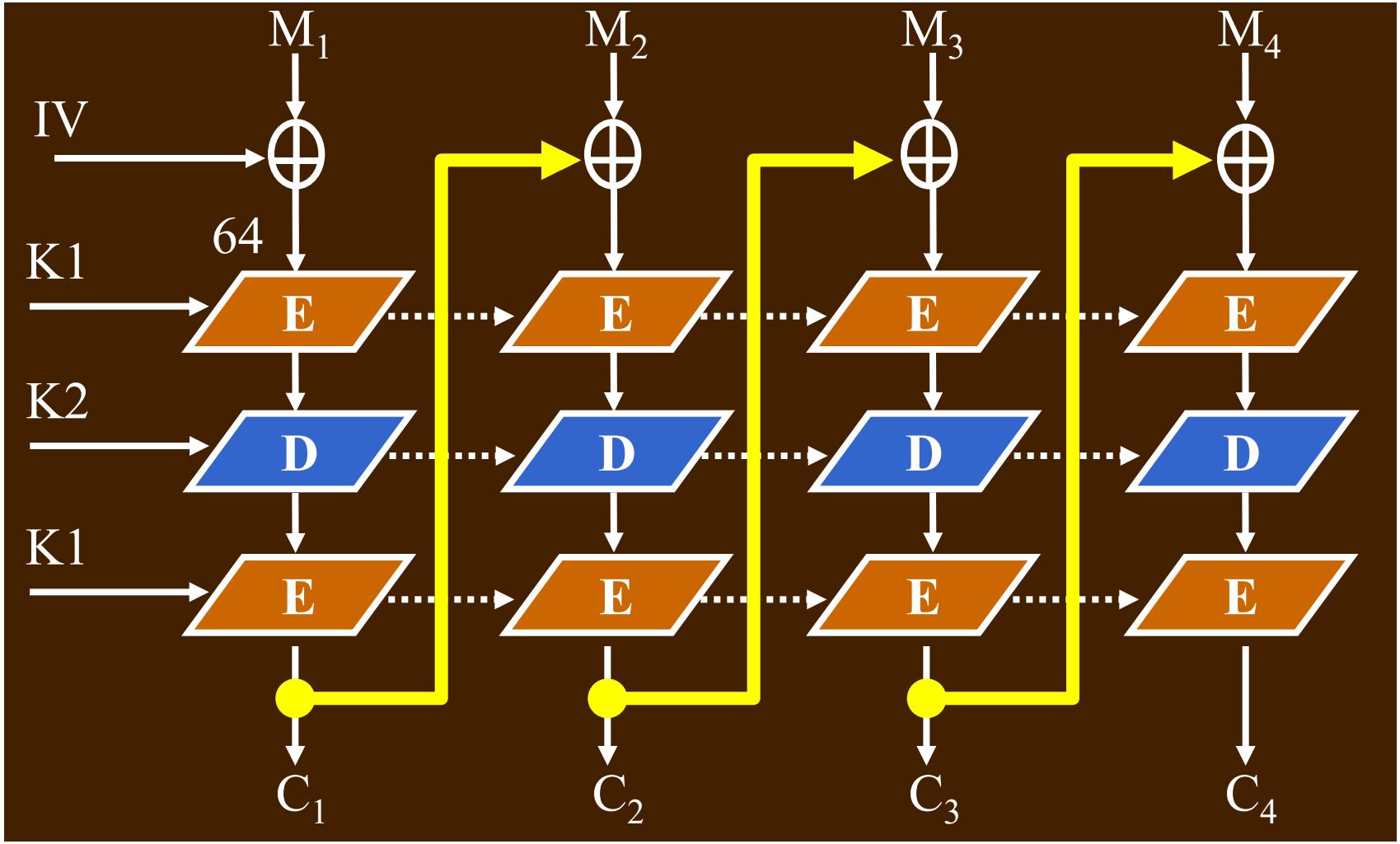
$X=D_{K_2}\{E_{K_1}\{P\}\}=D_{K_1}\{C\}$

TRIPLE DES (CONT'D)

- However: inefficient / expensive to compute
  - one third as fast as DES on the same platform, and DES is already designed to be slow in software

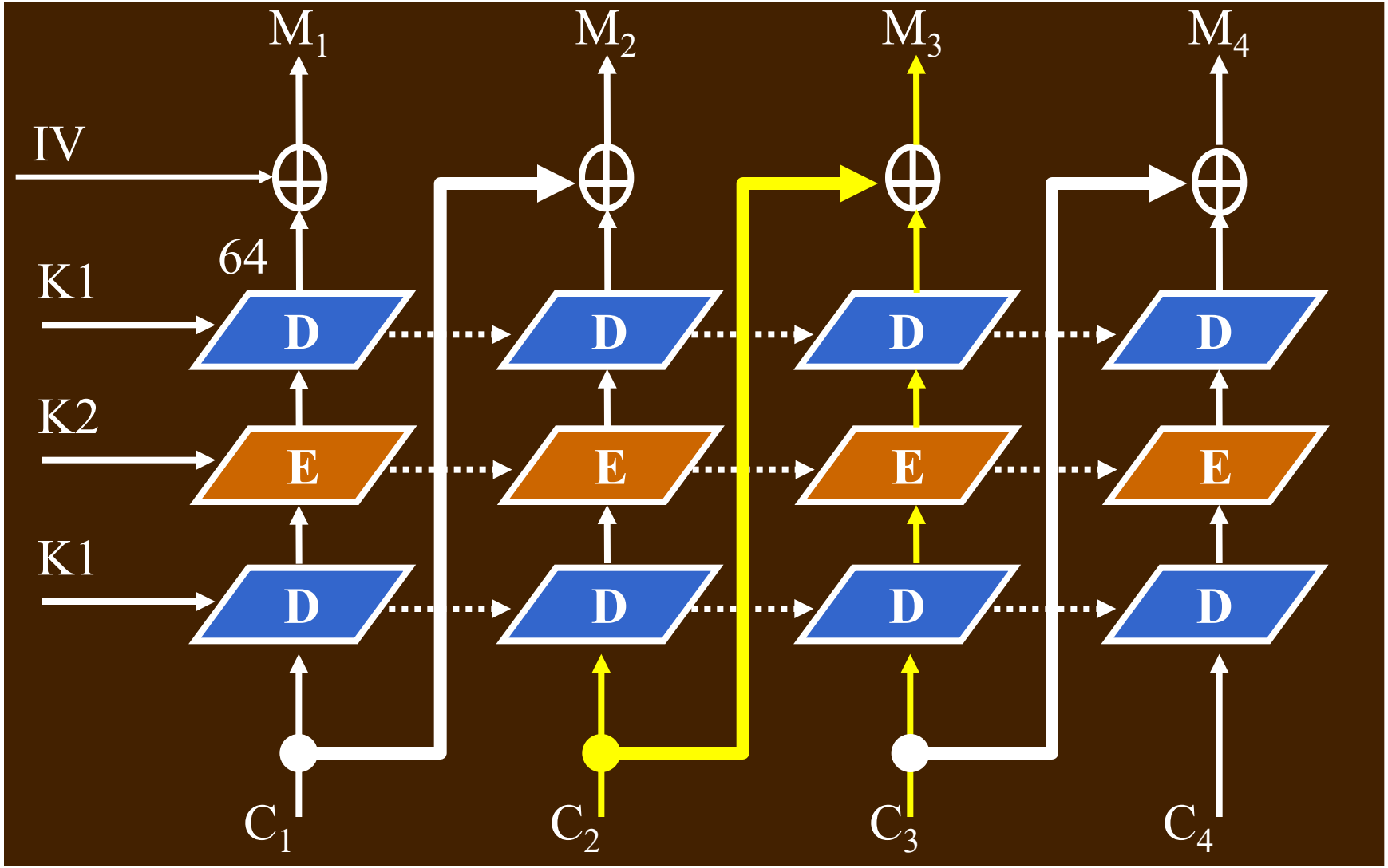
- Next question: how is block chaining used with triple-DES?

3DES-EDE: OUTSIDE CHAINING MODE

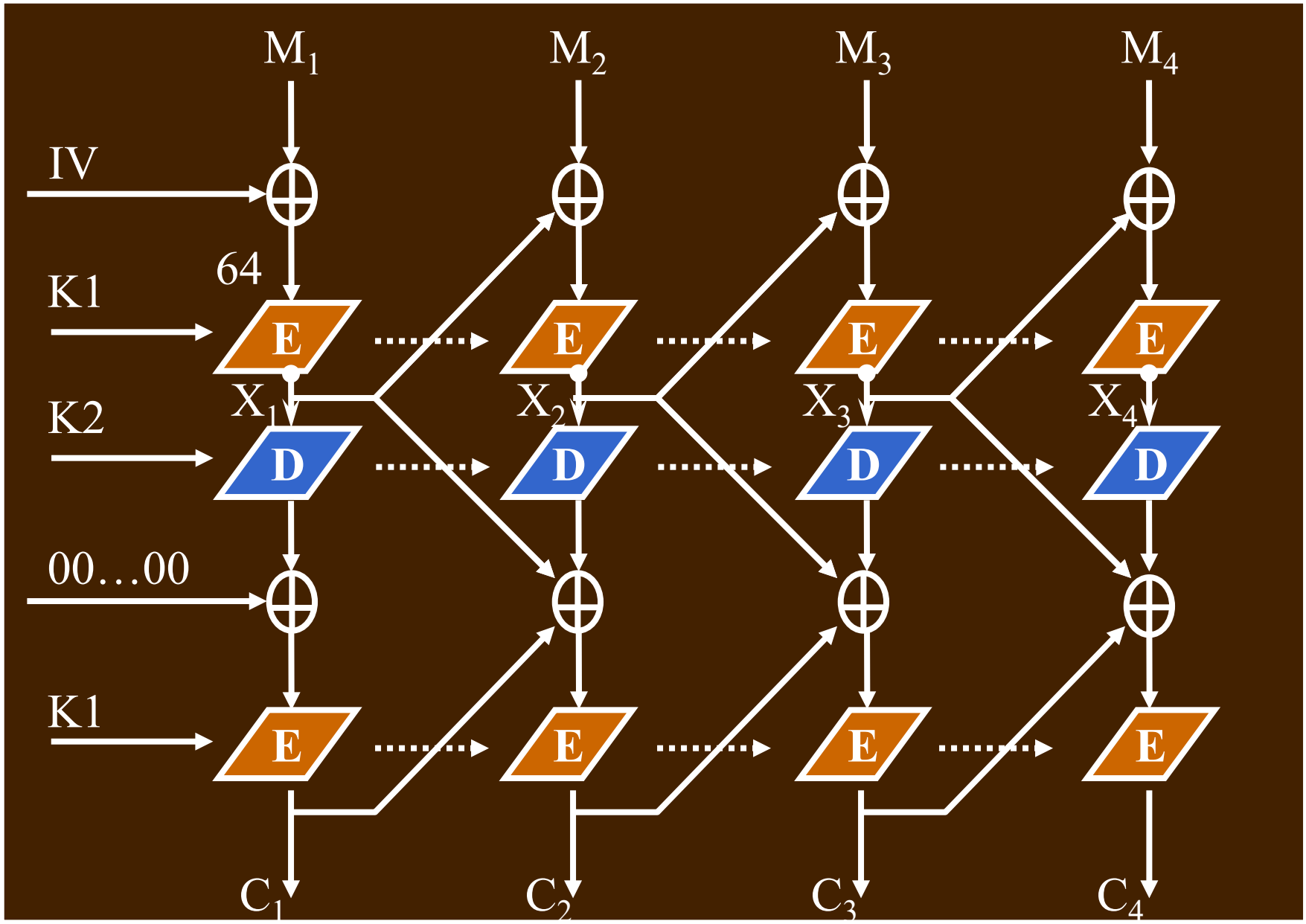


- What basic chaining mode is this?

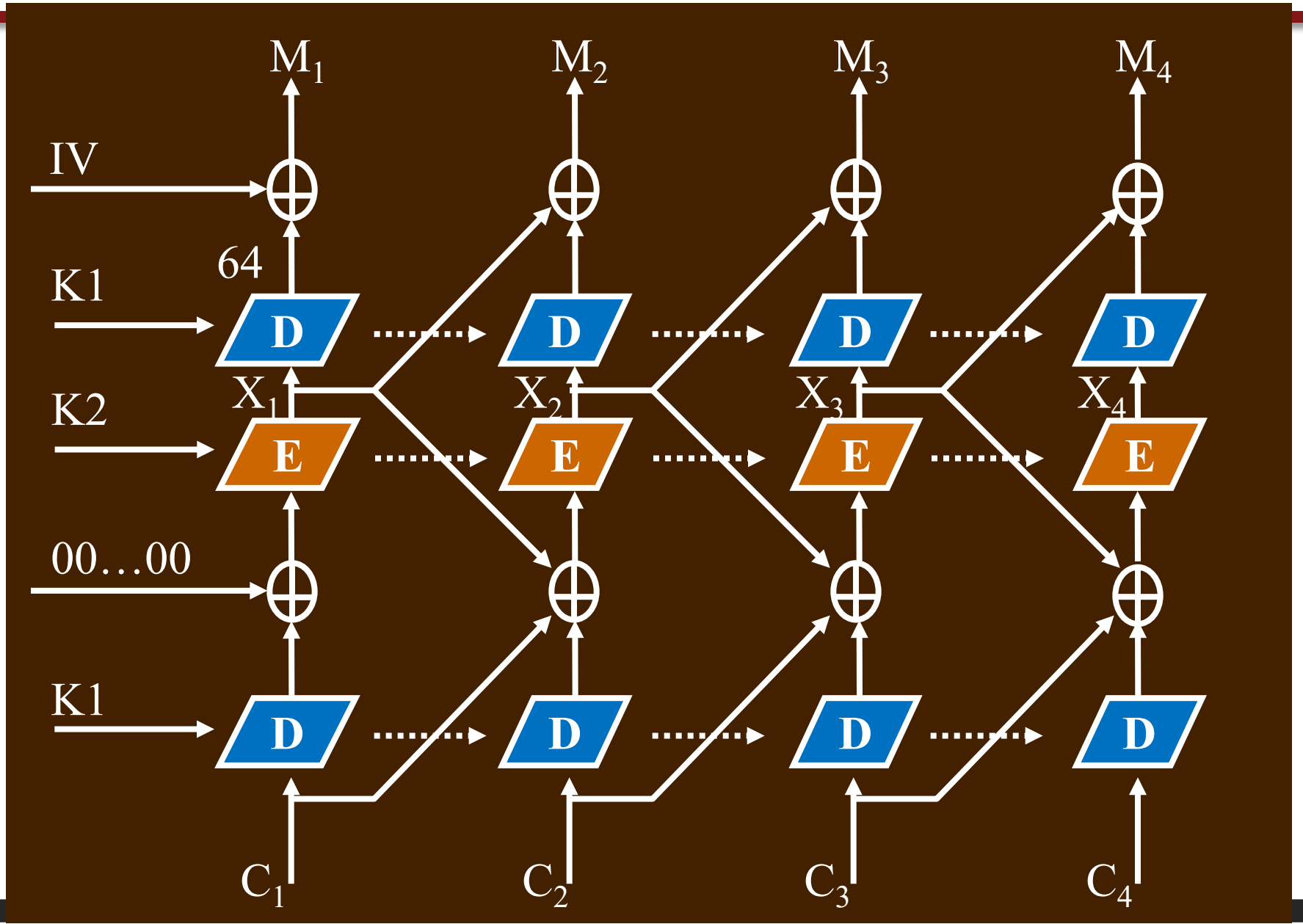
3DES-EDE: OCM DECRYPTION



3DES-EDE: INSIDE CHAINING MODE



3DES-EDE: ICM DECRYPTION



ICM PROPERTIES

- Does information leak?
  - identical plaintext blocks produce different ciphertext blocks
- Can ciphertext be manipulated?
  - hard
- Parallel processing possible?
  - no (encryption), partly (decryption)
- Do ciphertext errors propagate?
  - Yes