MAS 433: Cryptography

Lecture 7

Block Cipher (Part 4, Modes of Operation)

Wu Hongjun

Lecture Outline

- Classical ciphers
- Symmetric key encryption
  - One-time pad & information theory
  - Block cipher
    - DES, Double DES, Triple DES
    - AES
    - **Modes of Operation**
    - Attacks
  - Stream cipher
- Hash function and Message Authentication Code
- Public key encryption
- Digital signature
- Key establishment and management
- Introduction to other cryptographic topics

Recommended Reading

- CTP Section 3.7
- HAC Section 7.2.2
- Wikipedia:
  - Modes of operation

    http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation
  - Ciphertext Stealing

    http://en.wikipedia.org/wiki/Ciphertext_stealing

Block cipher

- Fixed block size
  - DES: 64 bits
  - AES: 128 bits
- How to encrypt many messages using the same key in a secure way?

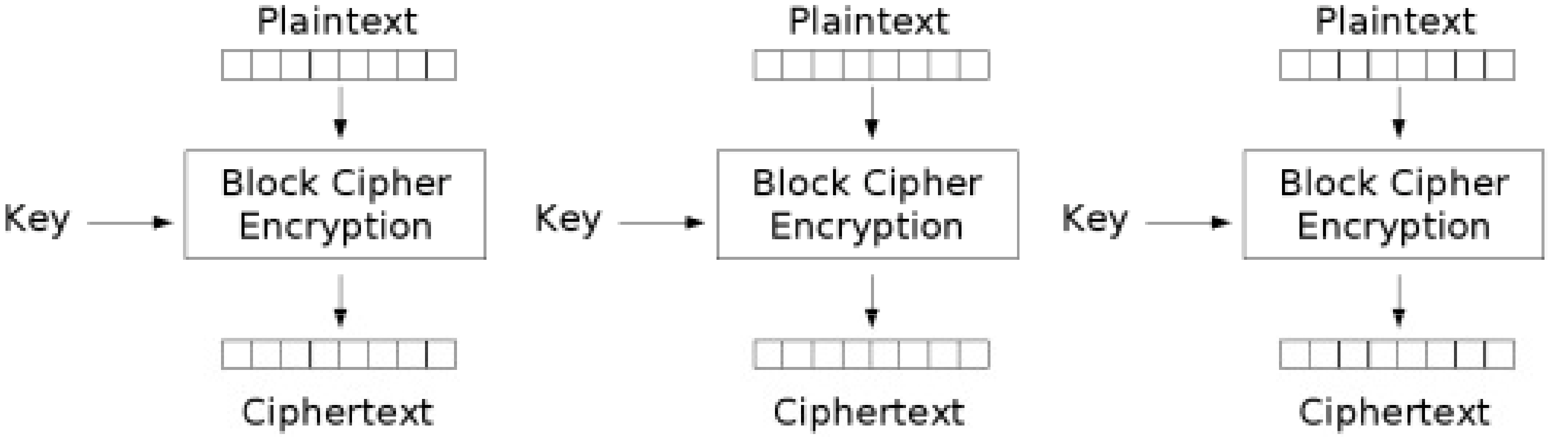
Block Cipher Modes of Operation

- NIST Special Publication 800-38A (2001)

  http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

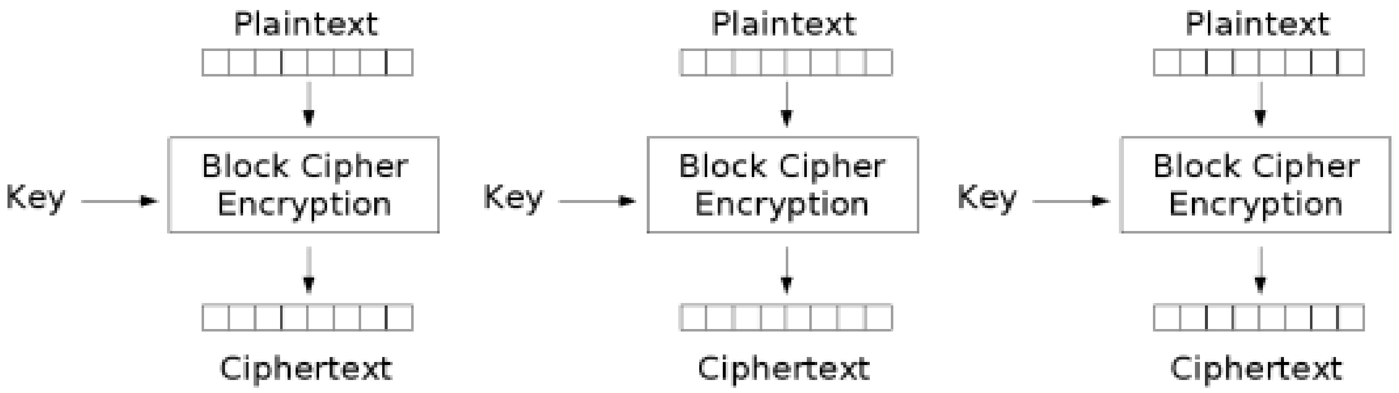
- Five encryption modes are recommended
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)

Electronic Codebook (ECB)



Electronic Codebook (ECB) mode encryption

Electronic Codebook (ECB)



Plaintext Plaintext Plaintext

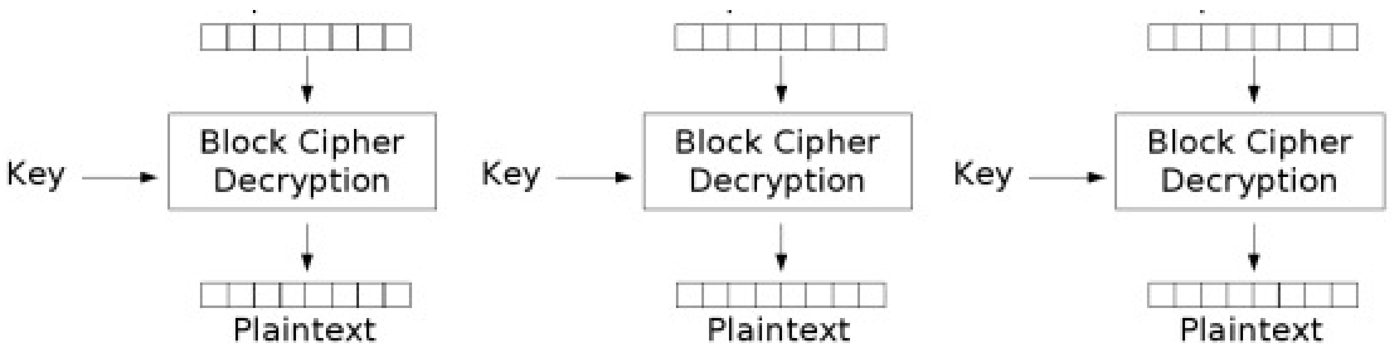
Key → Block Cipher Encryption

Key → Block Cipher Encryption

Key → Block Cipher Encryption

Ciphertext Ciphertext Ciphertext

Electronic Codebook (ECB) mode encryption



Key → Block Cipher Decryption

Key → Block Cipher Decryption

Key → Block Cipher Decryption

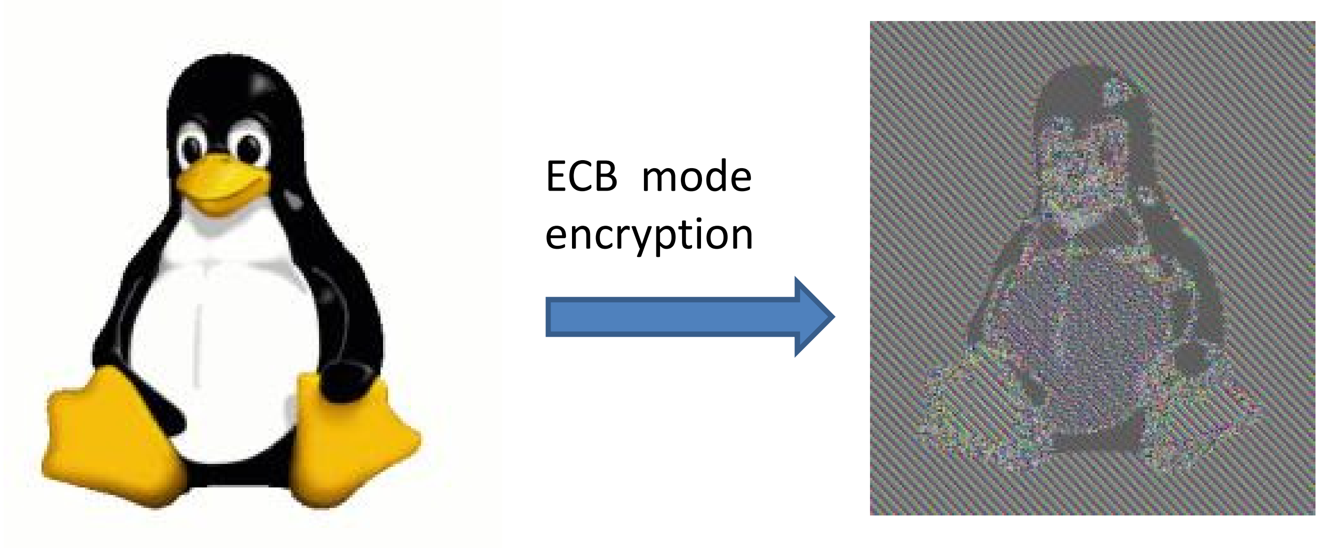
Plaintext Plaintext Plaintext

Electronic Codebook (ECB) mode decryption

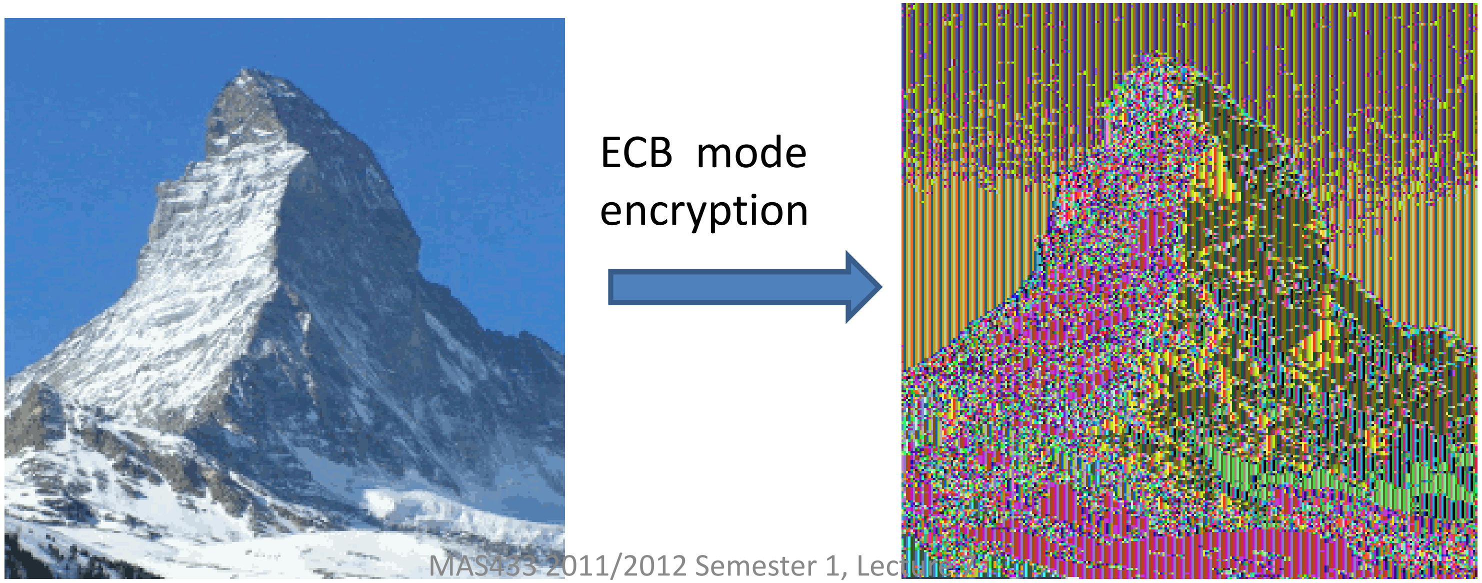
Electronic Codebook (ECB)

- ECB mode, same key + same plaintext block
  => the same ciphertext block
  - If this property is undesirable in an application, ECB mode should not be used
    - Example: Data with high redundancy
      - Uncompressed image file
    - Example: A secret key being used to encrypt too many data
      - there is a lot of redundancy in many documents, so the plaintext space in the ECB mode is limited
        - » Example: For AES, the input space size is 2^{128}. However, if each byte is used to represent an English letter, and if we assume that each letter carries about 1.5-bit information, then a 128-bit message block contains only about 16×1.5 = 24-bit information.

Electronic Codebook (ECB)



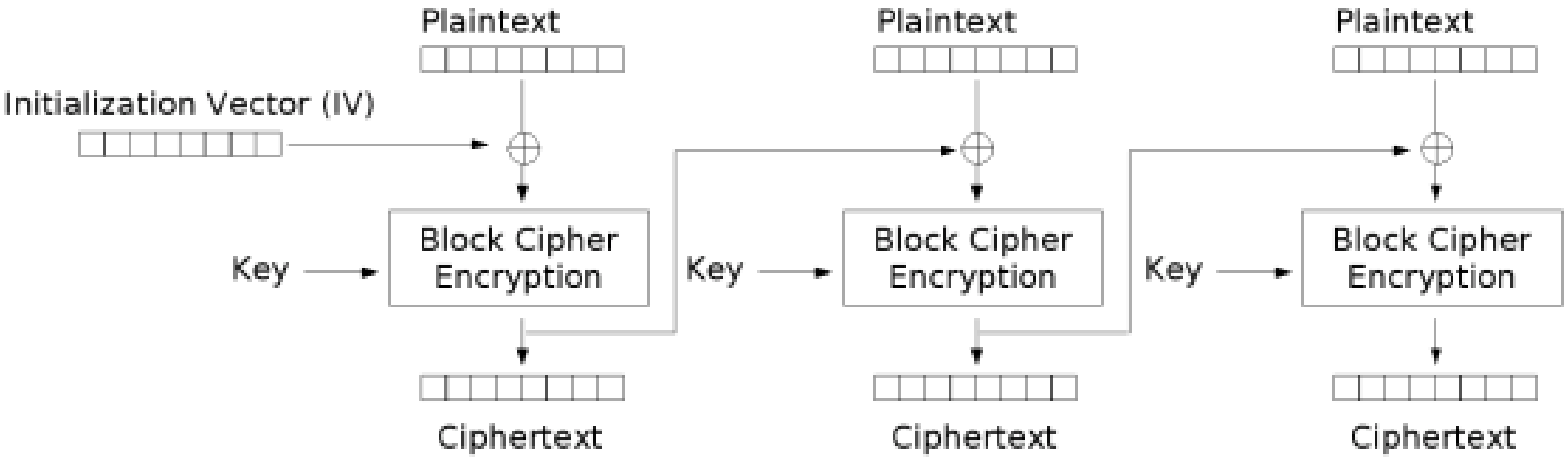
ECB mode encryption



ECB mode encryption

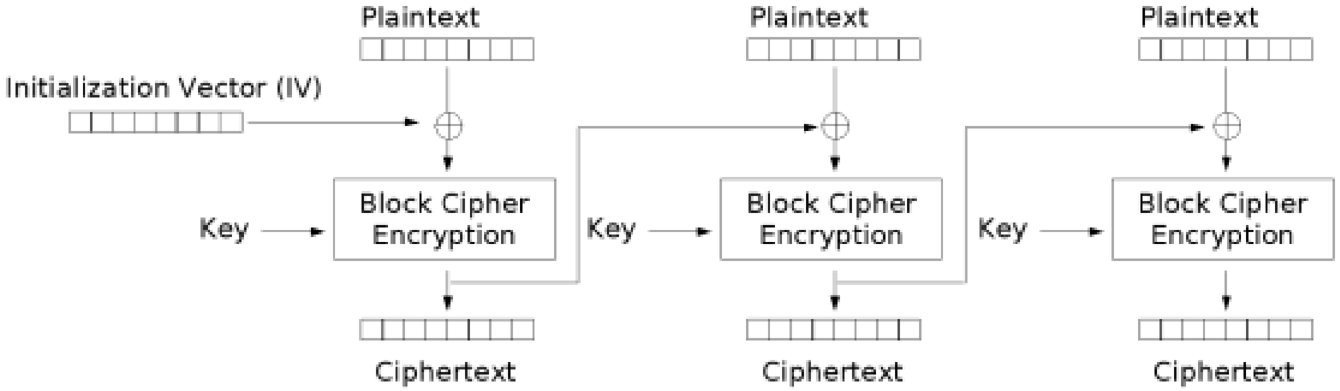
Cipher Block Chaining (CBC) Mode

- Invented by IBM in 1976
- Initialization vector (also called “nonce”)
  - need not be secret (normally sent/stored together with ciphertext)
  - but must be unpredictable for CBC mode

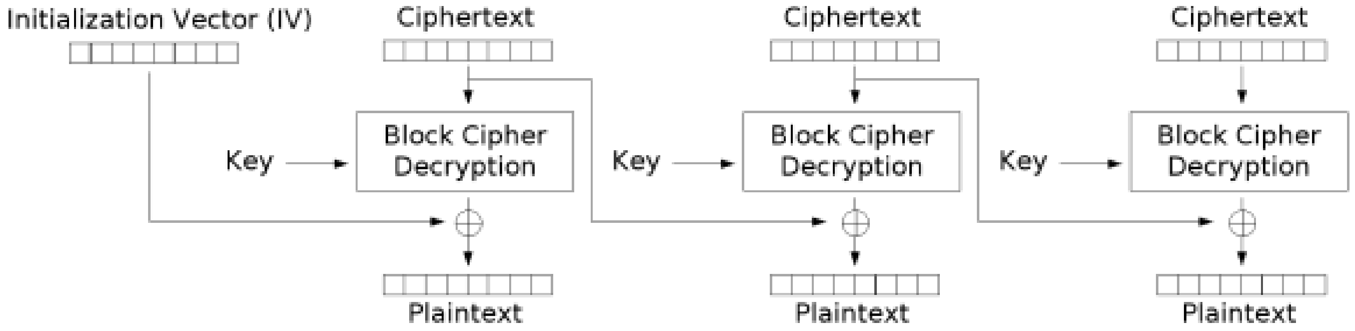


Cipher Block Chaining (CBC) mode encryption

Cipher Block Chaining (CBC) Mode



Cipher Block Chaining (CBC) mode encryption $C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$



Cipher Block Chaining (CBC) mode decryption $P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV$

Cipher Block Chaining (CBC) Mode

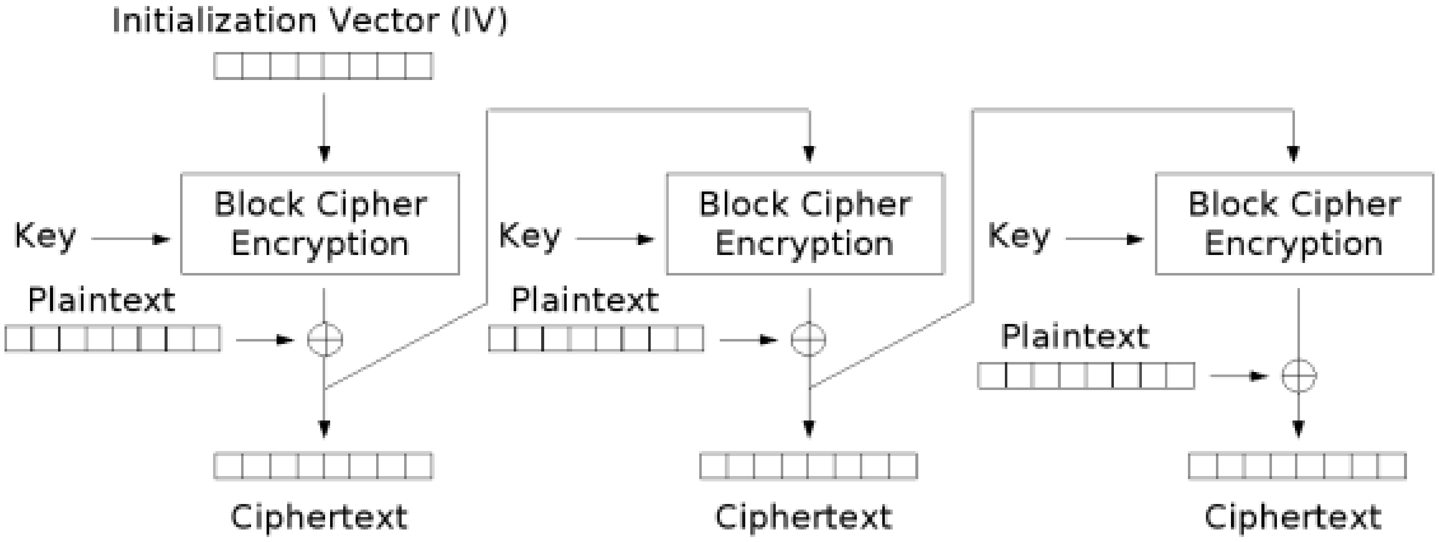
- CBC mode, the same key, the same plaintext block at different locations => different ciphertext blocks
  - The security of CBC is not that sensitive to the security of IV (If two IVs happen to be the same for the same key, encryption would not fail completely.)
    - The most reliable encryption mode!
    - The most commonly used encryption mode!

Cipher Feedback (CFB) Mode

- A simplified version of CFB:

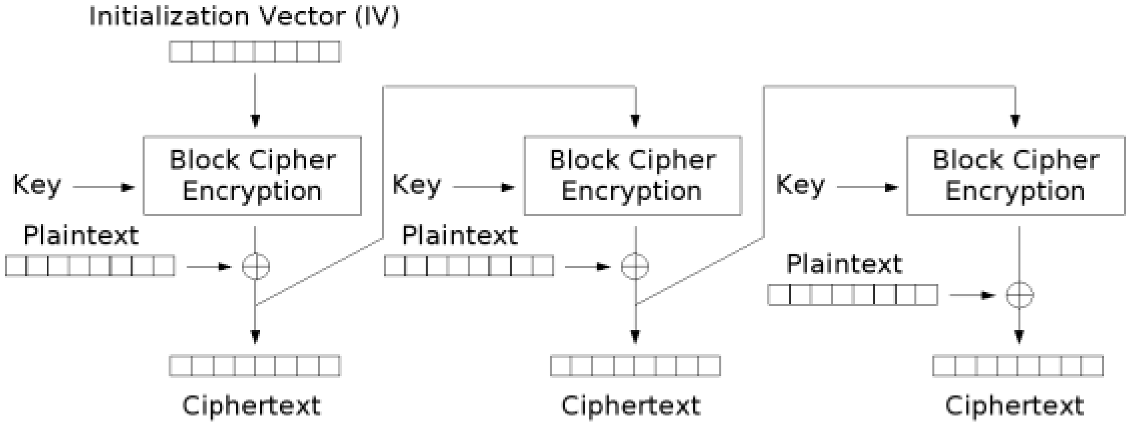
$$C_0 = \text{IV}$$

$$C_i = E_K(C_{i-1}) \oplus P_i$$



Cipher Feedback (CFB) mode encryption

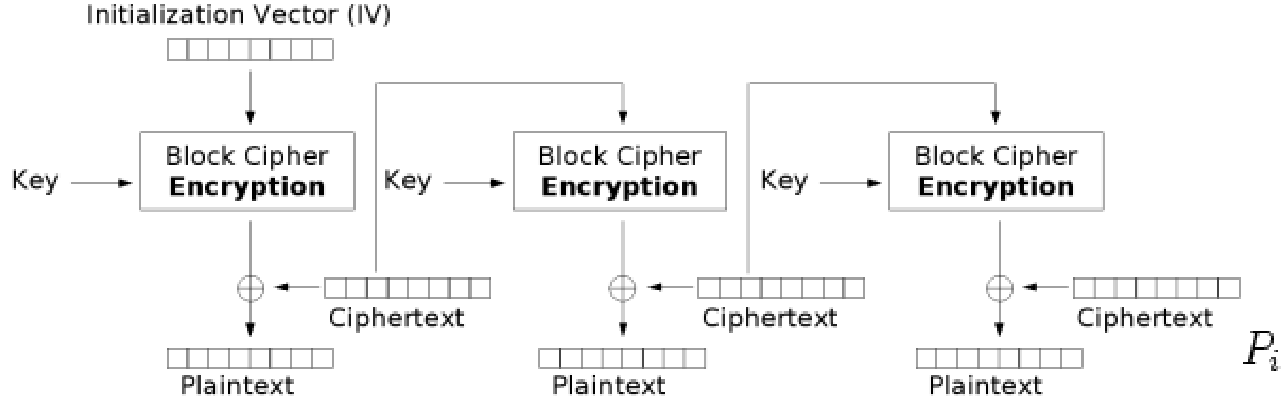
Cipher Feedback (CFB) Mode



$$C_0 = \mathrm{IV}$$

$$C_i = E_K(C_{i-1}) \oplus P_i$$

Cipher Feedback (CFB) mode encryption



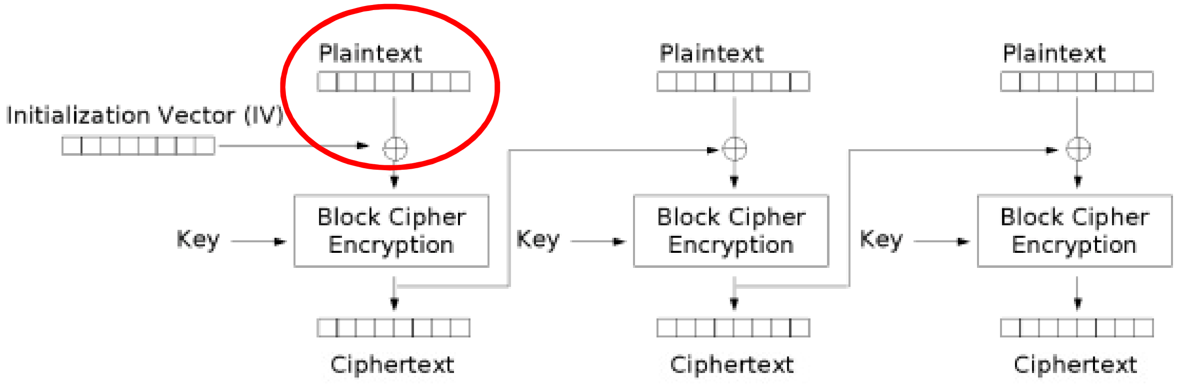
$$C_0 = \mathrm{IV}$$

$$P_i = E_K(C_{i-1}) \oplus C_i$$

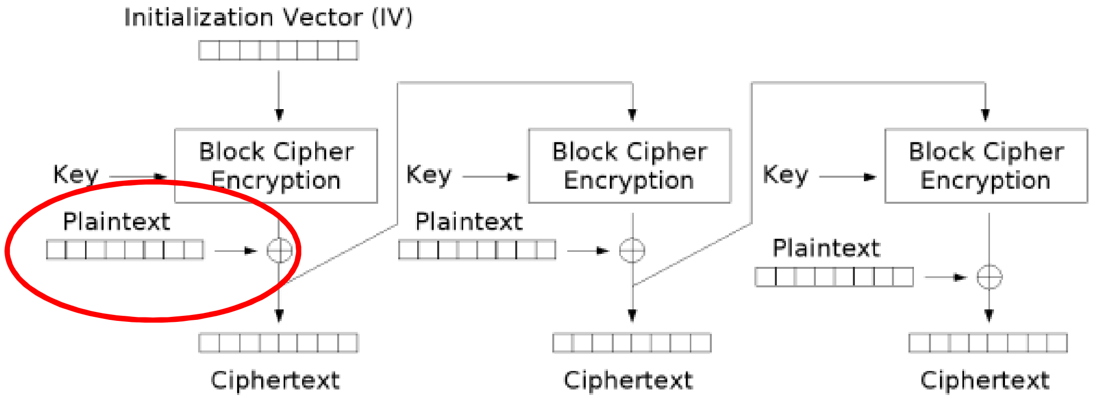
Cipher Feedback (CFB) mode decryption

Cipher Feedback (CFB) Mode

- Compare CBC & CFB



Cipher Block Chaining (CBC) mode encryption



Cipher Feedback (CFB) mode encryption

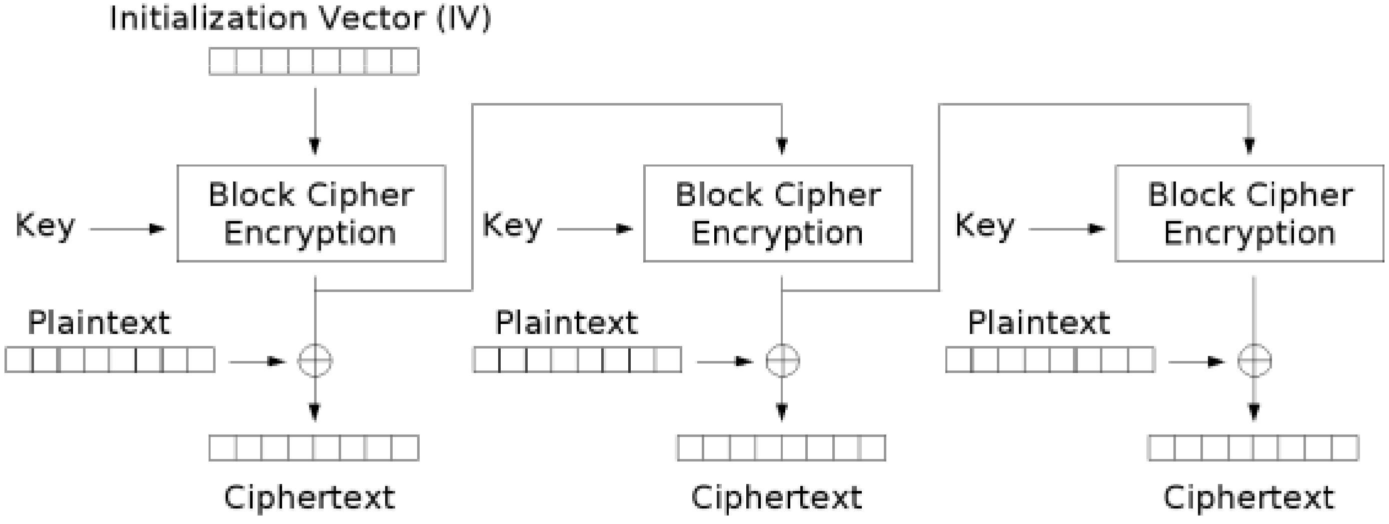
Similarity:
Each ciphertext block is used in the encryption of next block

Difference:
The plaintext

Output Feedback (OFB) Mode

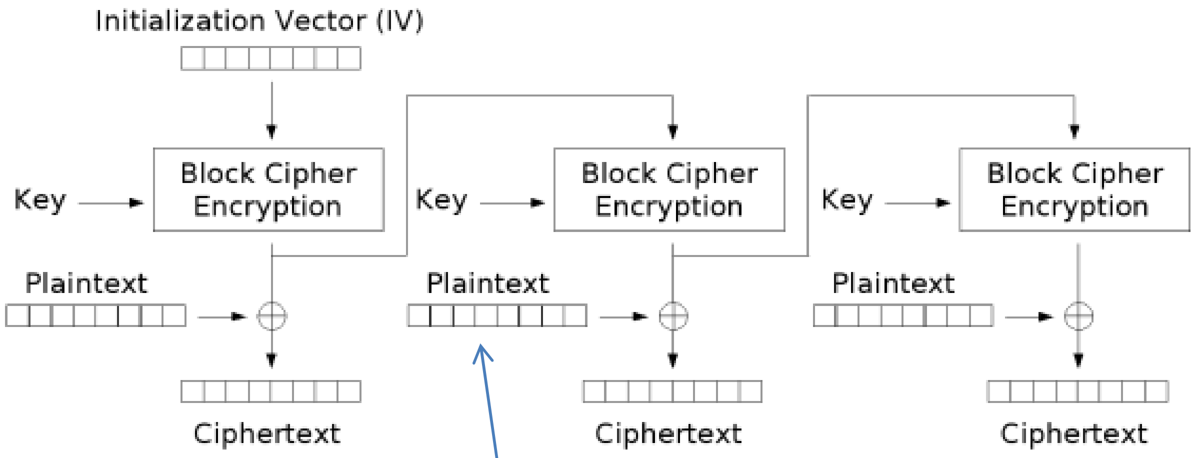
- A simplified version of OFB:

$$
\begin{aligned}
O_0 &= \text{IV} \\
O_i &= E_K(O_{i-1}) \\
C_i &= P_i \oplus O_i
\end{aligned}
$$

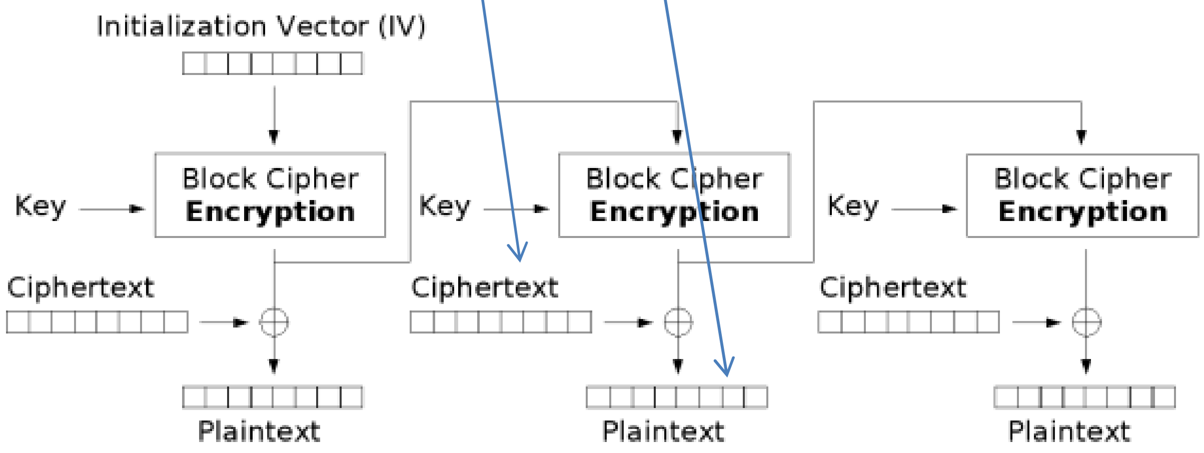


Output Feedback (OFB) mode encryption

Output Feedback (OFB) Mode



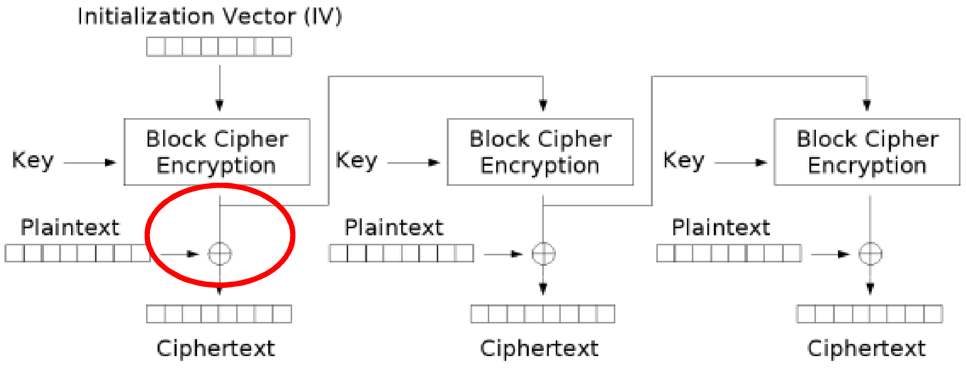
Output Feedback (OFB) mode encryption



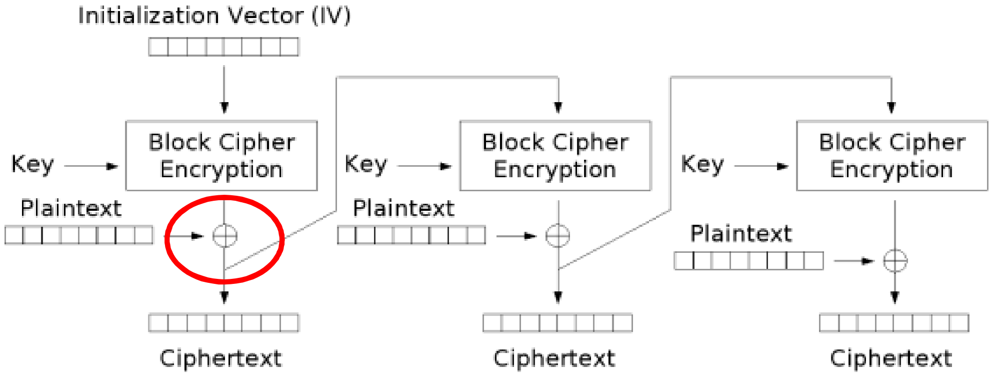
Output Feedback (OFB) mode decryption

Output Feedback (OFB) Mode

- Compare OFB & CFB



Output Feedback (OFB) mode encryption



Cipher Feedback (CFB) mode encryption

Counter (CTR) Mode

- For AES-CTR
  - The input of block cipher consists of 64-bit IV (nonce) and 64-bit counter
  - IV: different for each message,

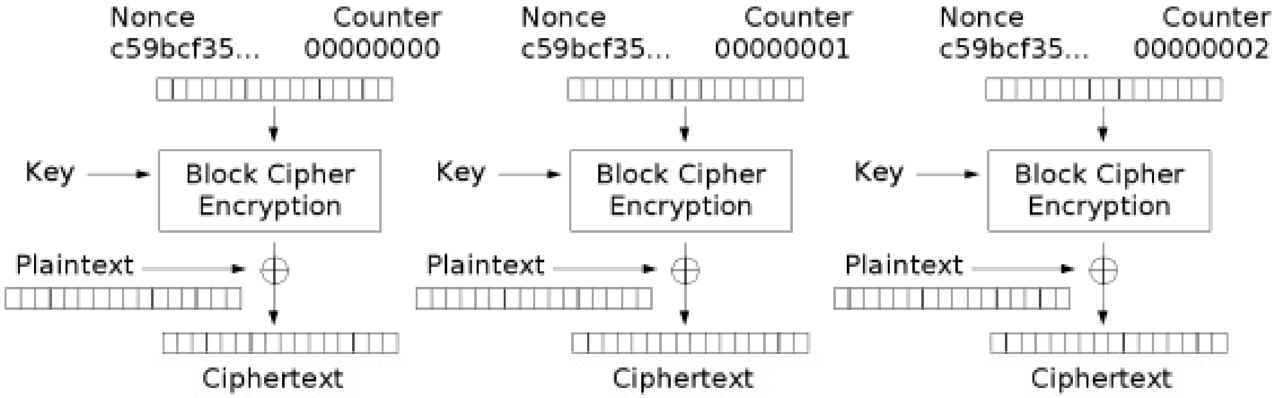
    remains the same for each message
  - Counter: start from 0,

    increased by 1 after each block

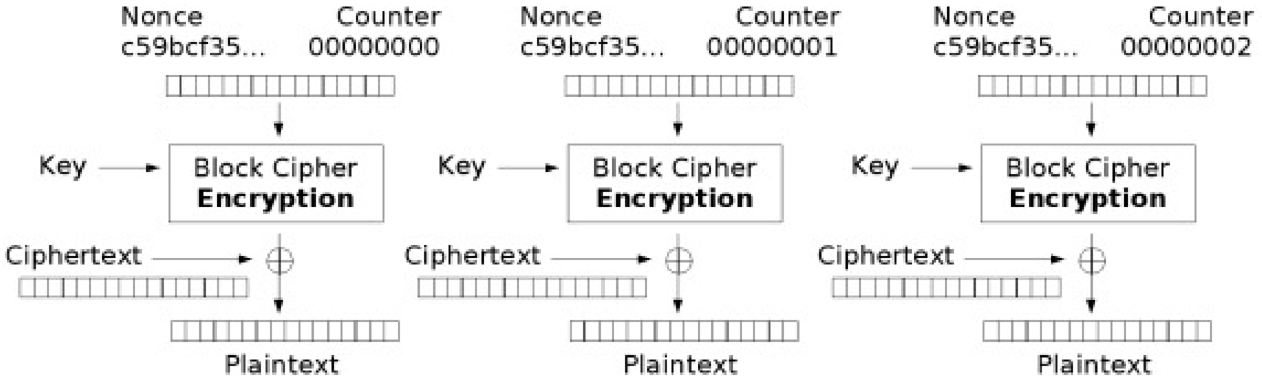
    perform the same way for each message

IV (64 bits)	Counter (64-bits)

Counter (CTR) Mode



Counter (CTR) mode encryption



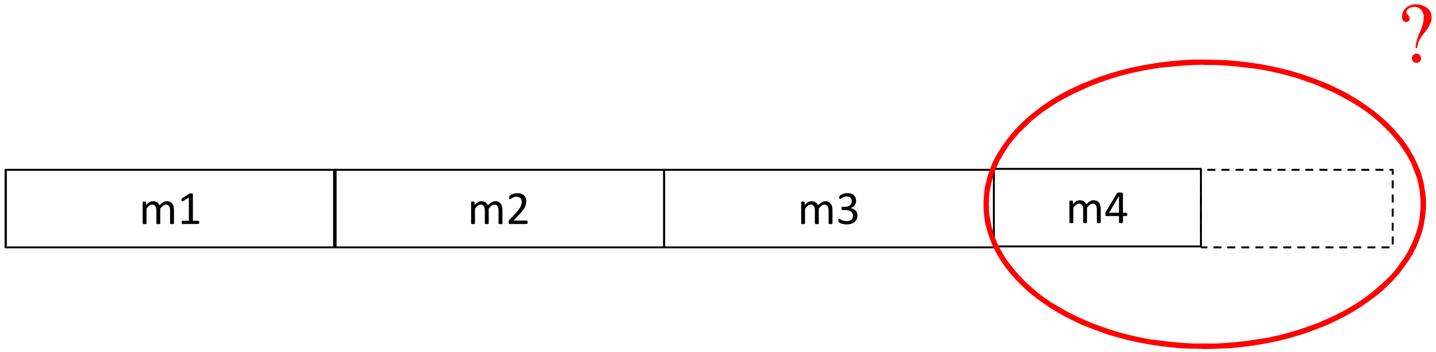
Counter (CTR) mode decryption

Counter (CTR) Mode

- For each message, the counter should not repeat
  - i.e., the length of each message for AES-CTR should not be more than 2^{64} blocks

How to encrypt a partial block?

- If the message length is not the multiple of the block size of the block cipher
  - the last block is called partial block



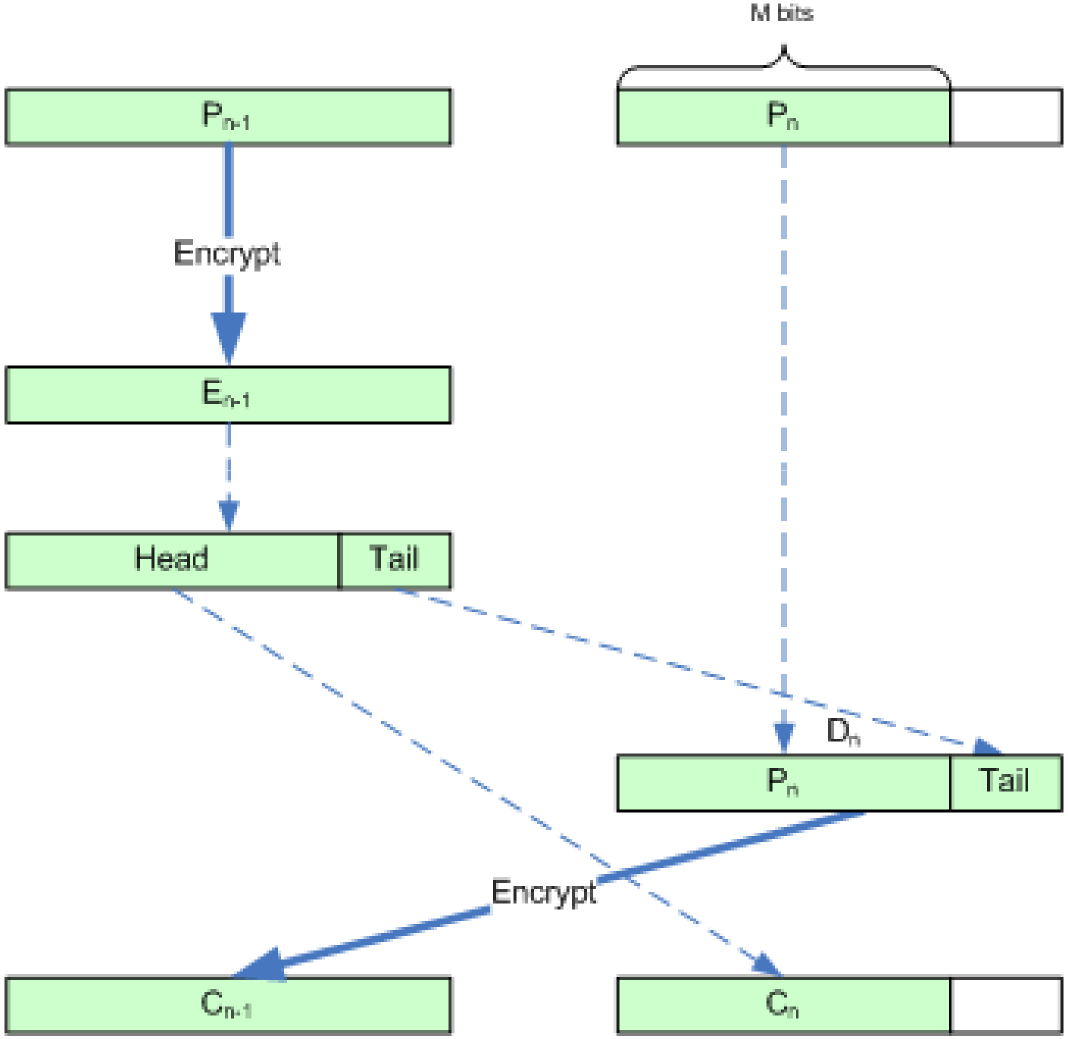
How to encrypt a partial block?

- ECB & CBC
  - Straightforward encryption:
    - Pad the partial block to full block
      - ECB: padded with random bits
        - » Otherwise, the entropy of the partial block may be too small
      - CBC: padded with random bits or constant bits
    - Ciphertext length larger than plaintext length
    - The actual message length is sent together with the ciphertext
- CFB, OFB, CTR
  - NO partial block problem
  - Why?

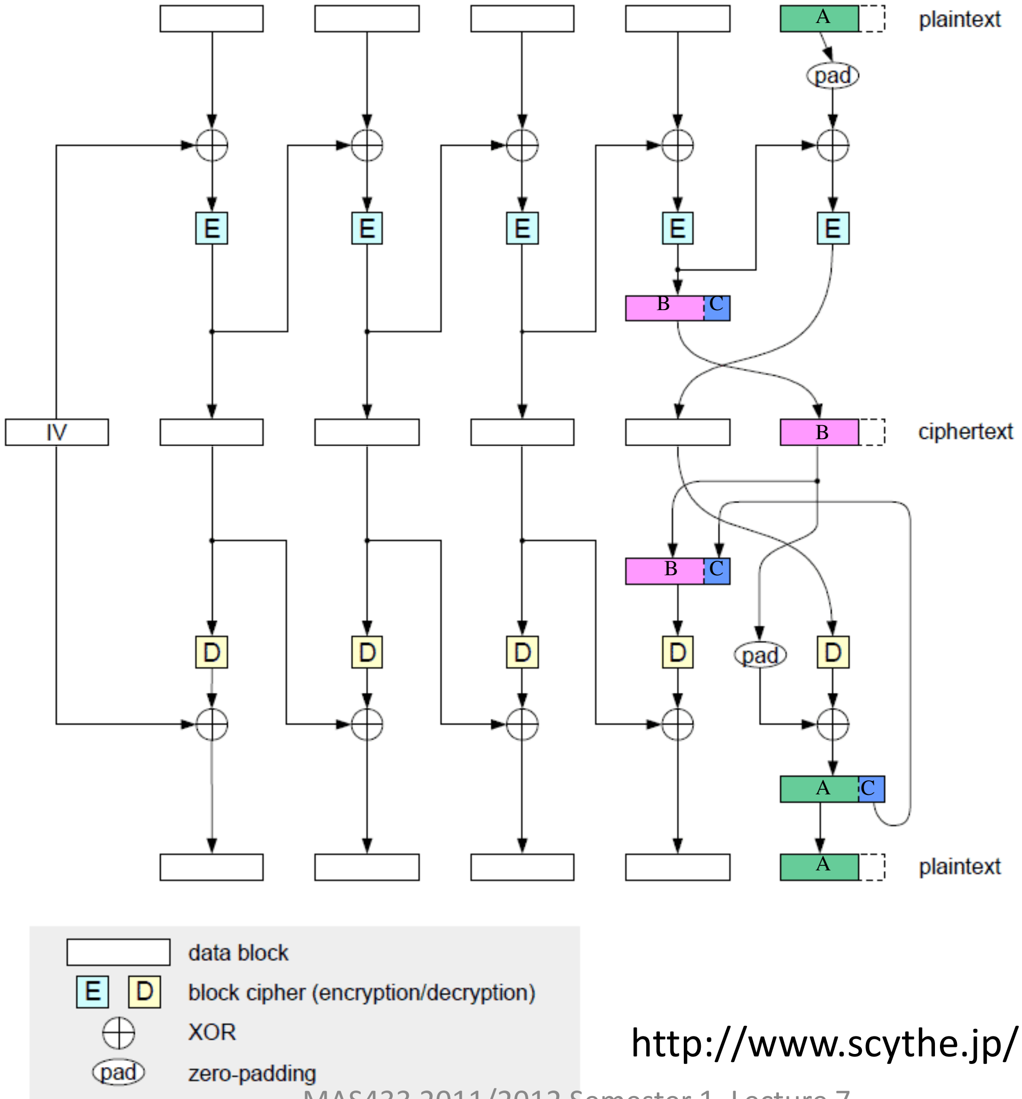
Ciphertext stealing

- Ciphertext stealing technique
  - Try to achieve:
    - Ciphertext length = Plaintext length
  - ECB ciphertext strealing
    - The plaintext should be more than one block
    - Otherwise, just use the padding method
  - CBC ciphertext strealing
    - Not necessary that plaintext is more than one block
      - If less than one full block, stealing from C_0 (IV).

ECB: Ciphertext Stealing



CBC: Ciphertext Stealing



http://www.scythe.jp/memo/crypto-cts.html

Summary

- Modes of operations
  - ECB: not strong
    - Parallel computation is possible
  - CBC: strong, the most commonly used
  - CFB
  - OFB: for the same key, all the IVs must be different
  - CTR: for the same key, all the IVs must be different
    - Parallel computation is possible
- Ciphertext stealing for encrypting the partial block
  - ECB
  - CBC
  - Not a problem for CFB, OFB & CTR