CYB 241 Digital Cryptography Techniques

Block Cipher Operation

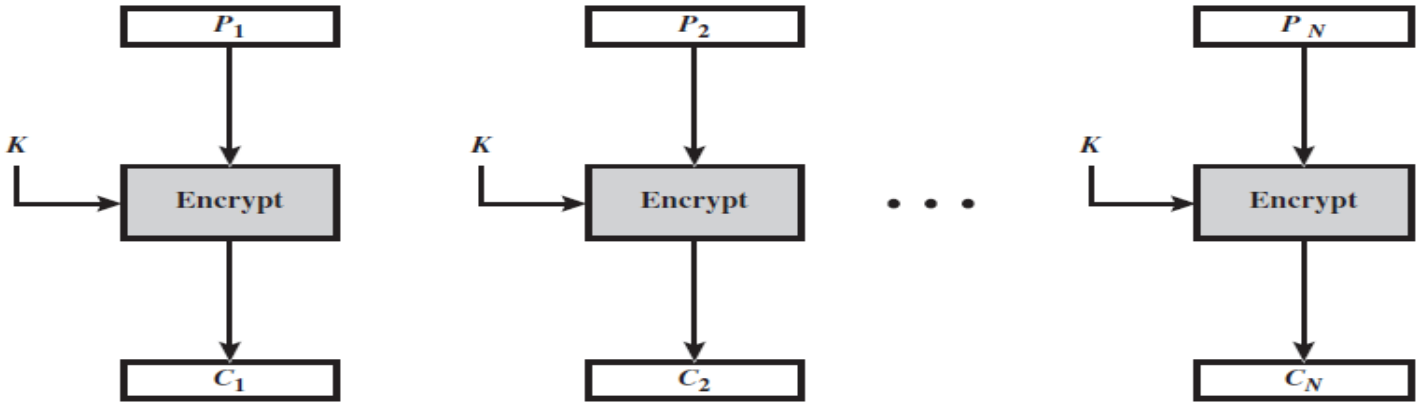
Block Cipher Modes of Operation

- Block cipher: operates on fixed length *b*-bit input to produce *b*-bit ciphertext
- What about encrypting plaintext longer than *b* bits?
- Break plaintext into *b*-bit blocks (padding if necessary) and apply cipher on each block
- Security issues arise: different modes of operation have been developed
  - Each is suitable for certain applications
  - They can be used with any symmetric block cipher, including triple DES and AES

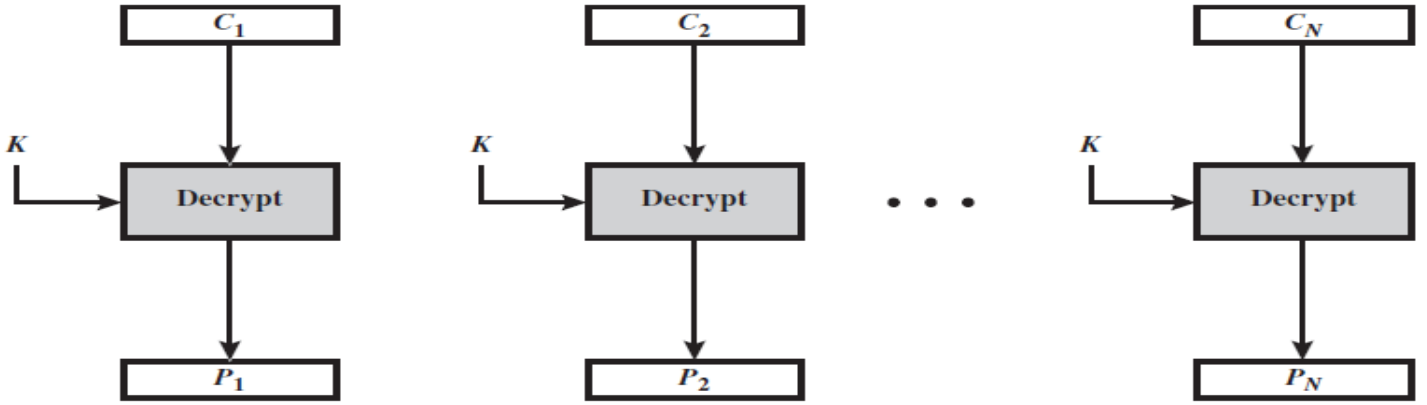
Electronic Codebook Mode (ECB)

- Break message into b-bit blocks (e.g. 64) and padding the last block if needed.
- Encrypt each block independently
- Suitable for short amount of data (e.g. key)
- Identical P blocks produce same C blocks
- Regularities appear in long, structured messages
- Cryptanalysis is possible

Electronic Codebook Mode (ECB)



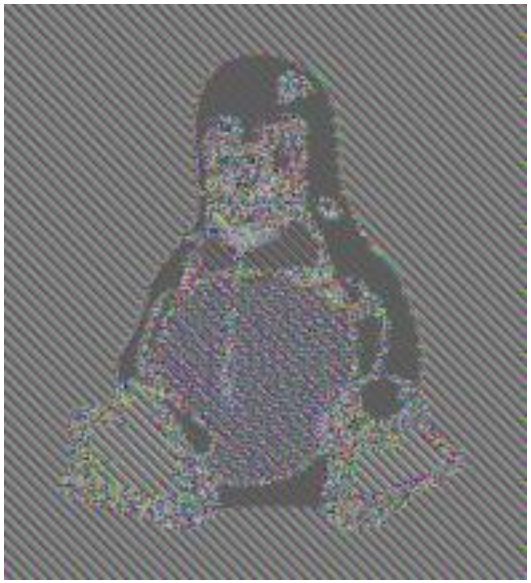
(a) Encryption



(b) Decryption

Electronic Codebook Mode*

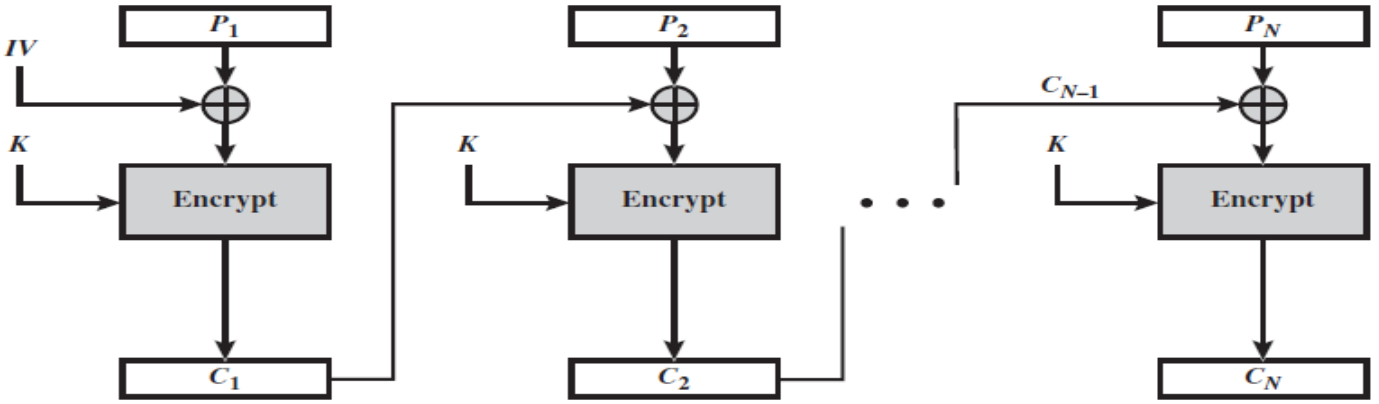
Original image



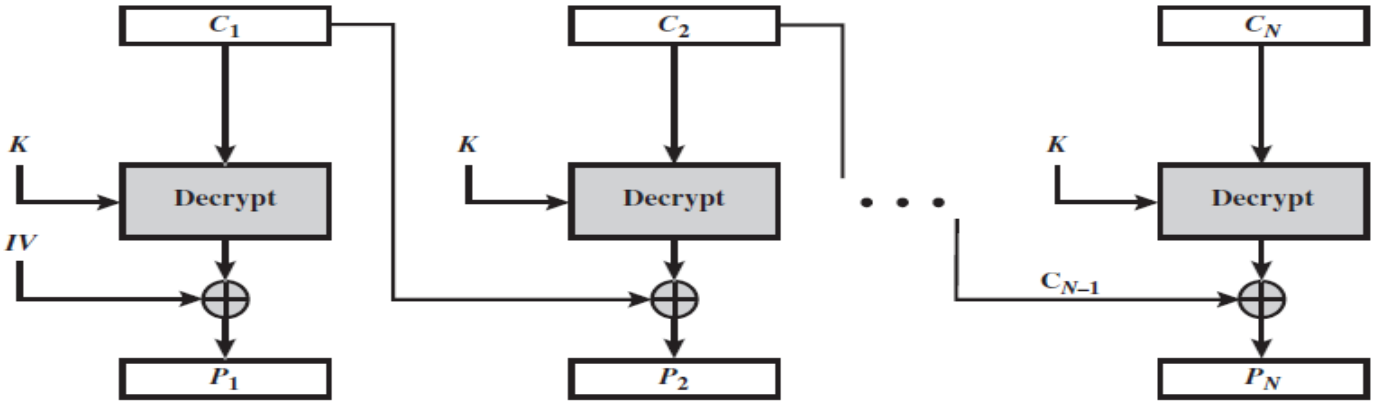
Encrypted using ECB mode

* https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Cipher Block Chaining Mode (CBC)



(a) Encryption

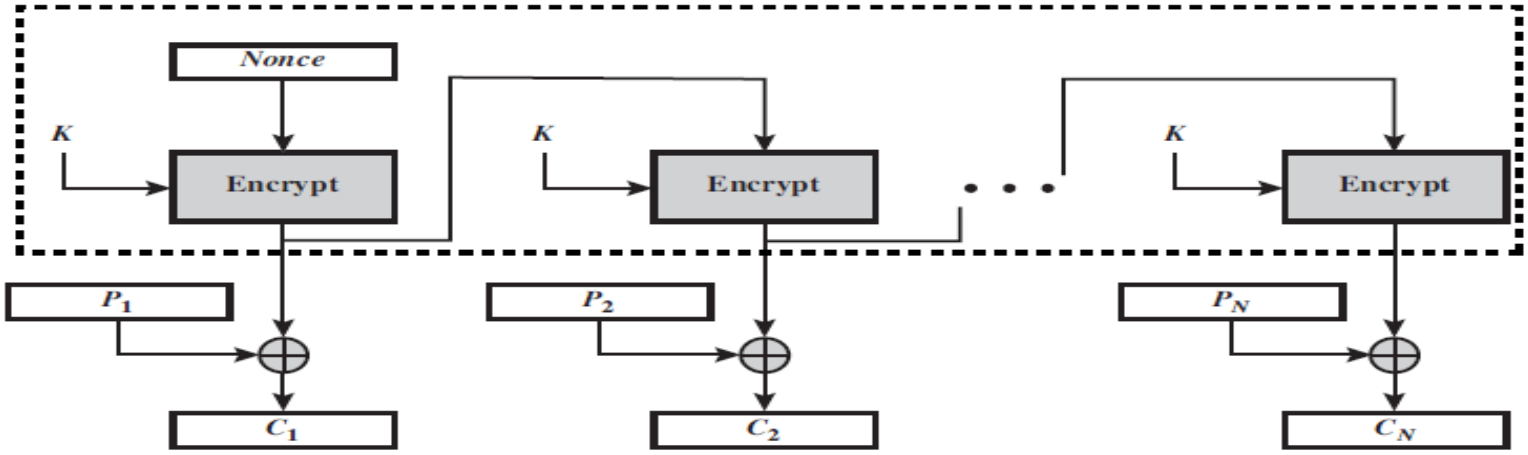


(b) Decryption

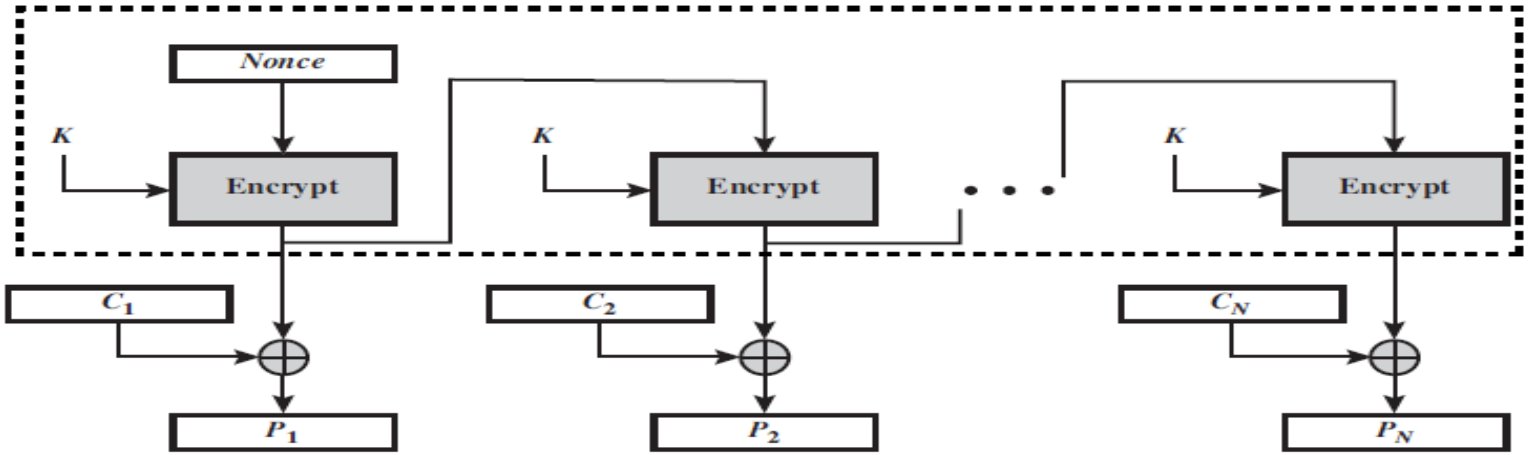
Cipher Block Chaining Mode (CBC)

- Break message into b-bit blocks (e.g. 64) and padding the last block if needed.
- Before encryption, XOR current P block and previous C block
- The first block XORed with Initial Vector (IV)
- Identical P blocks produce different C blocks
- Suitable for long messages
- IV must be known to both sides and can be encrypted using ECB mode
- CBC also in message authentication

Output Feedback Mode (OFB)



(a) Encryption

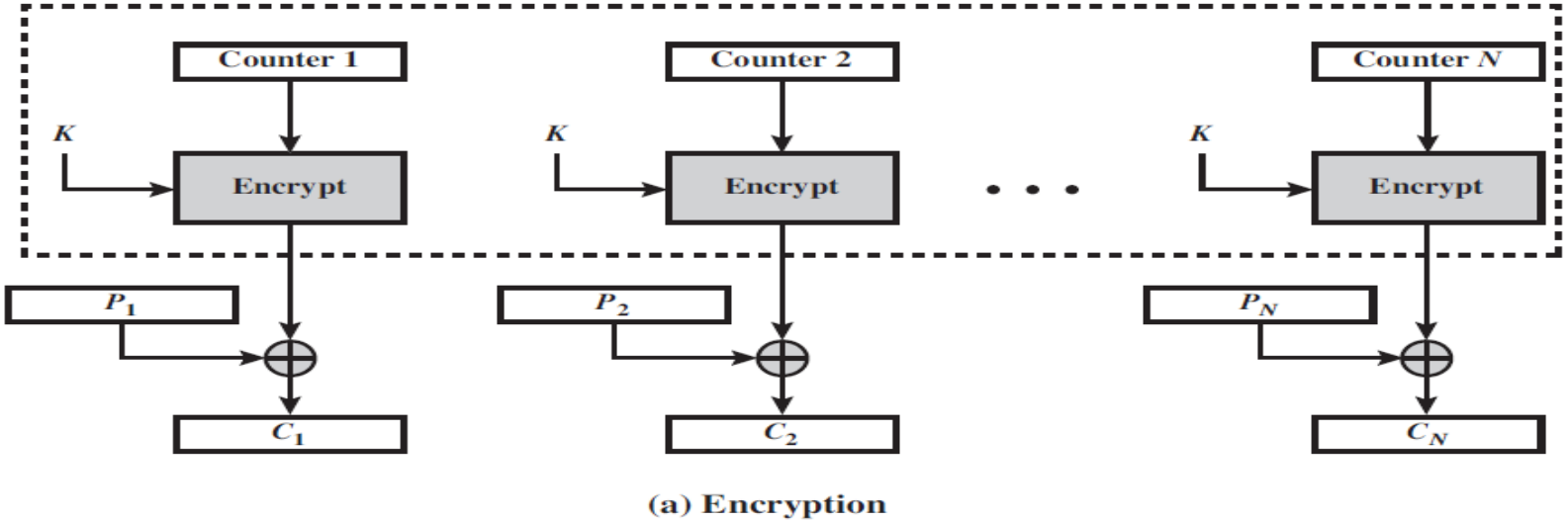


(b) Decryption

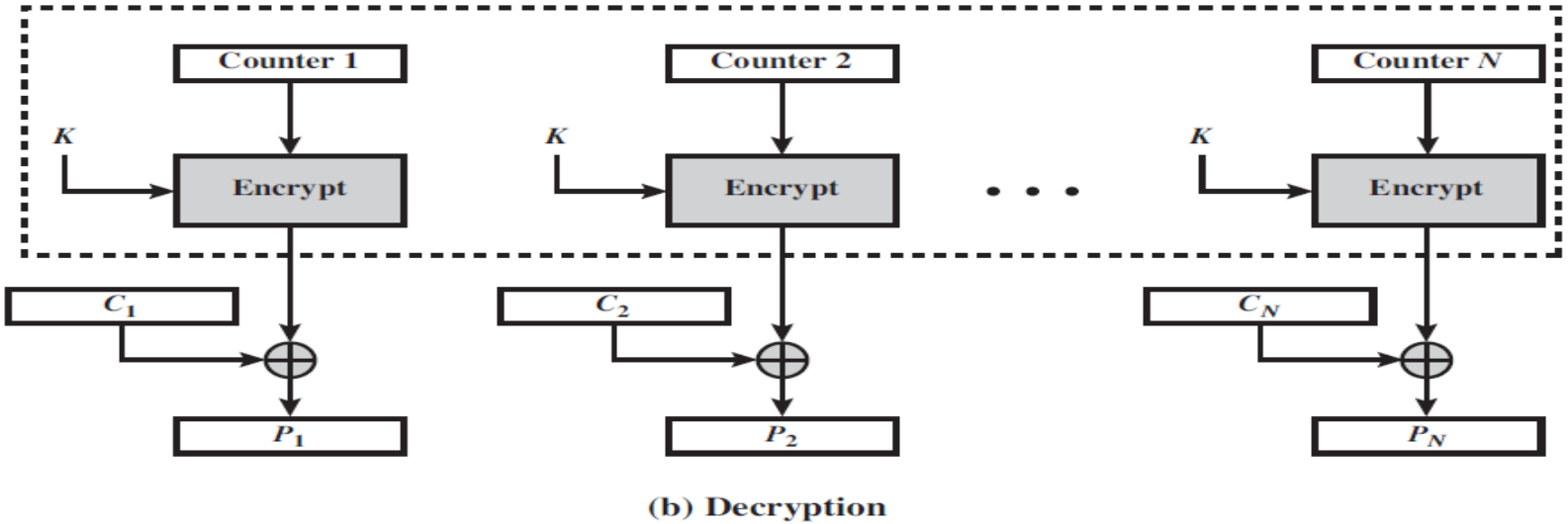
Output Feedback Mode (OFB)

- Output of encryption (not C_i) is fed back
- Operates on full blocks of P and C
- Bit errors in transmission do not propagate.
- The output of encryption function depends on the key and an initial value and independent of the plaintext

Counter Mode (CTR)



(a) Encryption



(b) Decryption

Counter Mode (CTR)

- Counter with b-bits (block size of E) is used
- Counter value must be different for each P
- Counter value initialized to certain value
- Counter incremented for each subsequent P
- Encryption: $C_i = P_i \oplus E(K, \text{Counter})]$
- Decryption: $P_i = C_i \oplus E(K, \text{Counter})]$
- No chaining is used

Counter Mode Advantages

- Hardware efficiency
  - no chaining, blocks encrypted in parallel
- Software efficiency
  - parallel processing can be used
- Preprocessing
  - output of E can be pre-computed & stored
- Random access
  - i^{th} block of plain/cipher text can be processed randomly
- Provable security
- Simplicity
  - only encryption algorithm is needed

Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	•General-purpose block-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

Reading Assignment

- Textbook
  - chapter 7
    - 7.1
    - 7.2
    - 7.3
    - 7.4
    - 7.5
    - 7.6