CS8792 Cryptography and Network Security

Block cipher: modes of operation

Unit-II

September 10, 2020

Session Objectives

- Different modes of operations

Session Outcomes

At the end of this session, participants will be able to

- Discuss various modes of block cipher operations

Agenda

Presentation Outline

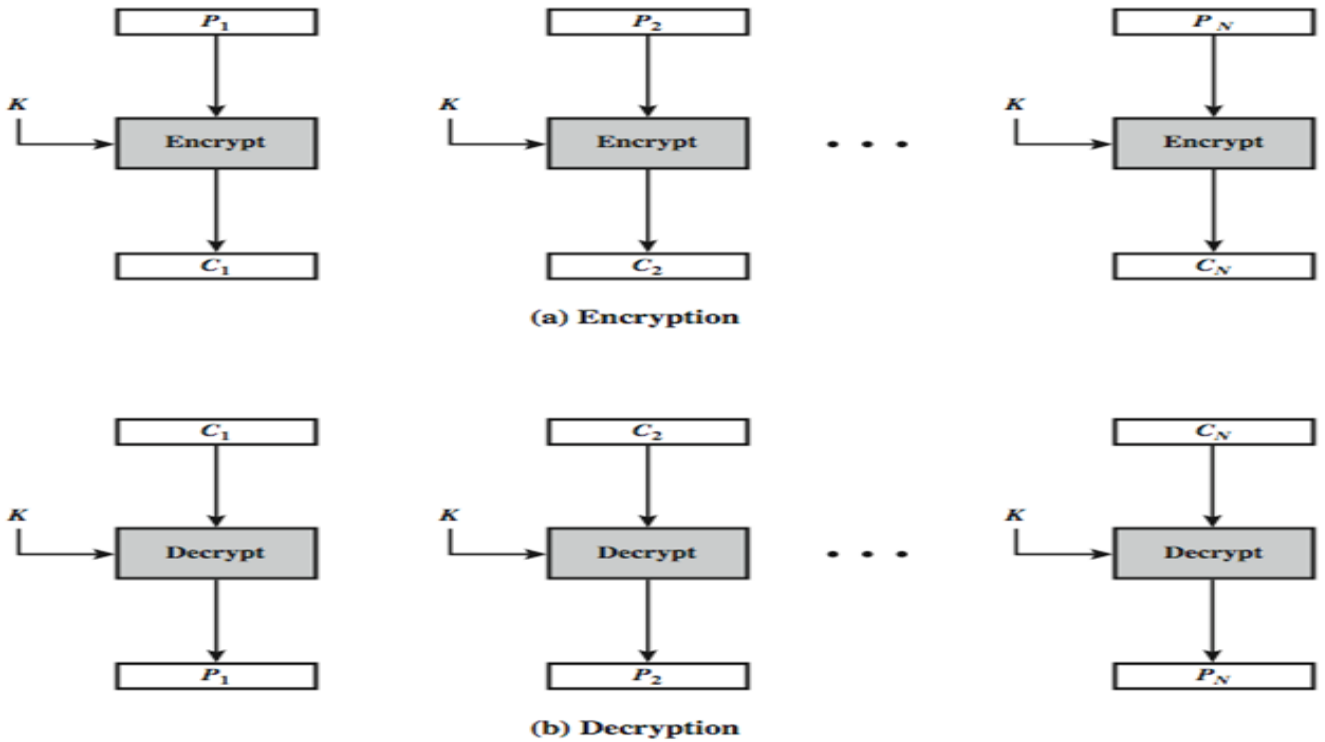
Modes of Operation

- Block ciphers encrypt fixed size blocks e.g., DES encrypts 64-bit blocks
- Need some way to en/decrypt arbitrary amounts of data in practice
- NIST SP 800-38A defines 5 modes
- Have block and stream modes
- To cover a wide variety of applications
- Can be used with any block cipher

Electronic Codebook Book (ECB)

- Message is broken into independent blocks that are encrypted
- Each block is a value which is substituted, like a codebook, hence name
- Each block is encoded independently of the other blocks $C_i = E_K(P_i)$
- Uses: secure transmission of single values

ECB


P_1
P_2
P_N
K
Encrypt
C_1
C_2
C_N
(a) Encryption
C_1
C_2
C_N
K
Decrypt
P_1
P_2
P_N
(b) Decryption

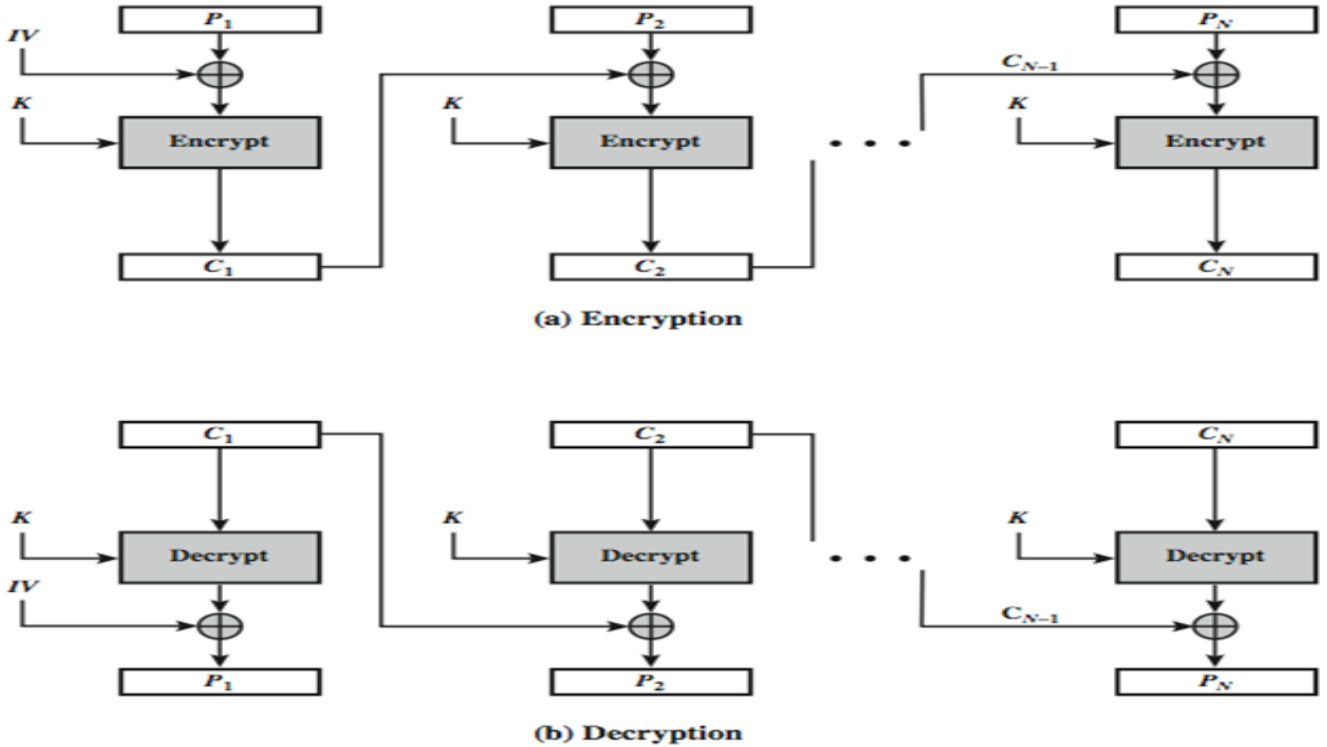
Advantages and Limitations of ECB

- message repetitions may show in ciphertext
  - if aligned with message block
  - particularly with data such graphics
  - or with messages that change very little, which become a code-book analysis problem
- weakness is due to the encrypted message blocks being independent
- vulnerable to cut-and-paste attacks
- main use is sending a few blocks of data

Cipher Block Chaining (CBC)

- message is broken into blocks
- linked together in encryption operation
- each previous cipher block is chained with current plaintext block, hence name
- use Initial Vector (IV) to start process
  $C_i = E_K(P_i \oplus C_{i-1})$
  $C_{-1} = \text{IV}$
- IV prevents same P from making same C
- uses: bulk data encryption, authentication

CBC


IV
K
Encrypt
P_1
C_1
P_2
C_2
C_{N-1}
P_N
C_N
(a) Encryption
Decrypt
(b) Decryption

Advantages and Limitations of CBC

- a ciphertext block depends on all blocks before it
- any change to a block affects all following ciphertext blocks
- need Initialization Vector (IV) which must be known to sender & receiver
- if sent in clear, attacker can change bits of first block, by changing corresponding bits of IV
  - hence IV must either be a fixed value
  - or derived in way hard to manipulate
  - or sent encrypted in ECB mode before rest of message
  - or message integrity must be checked otherwise

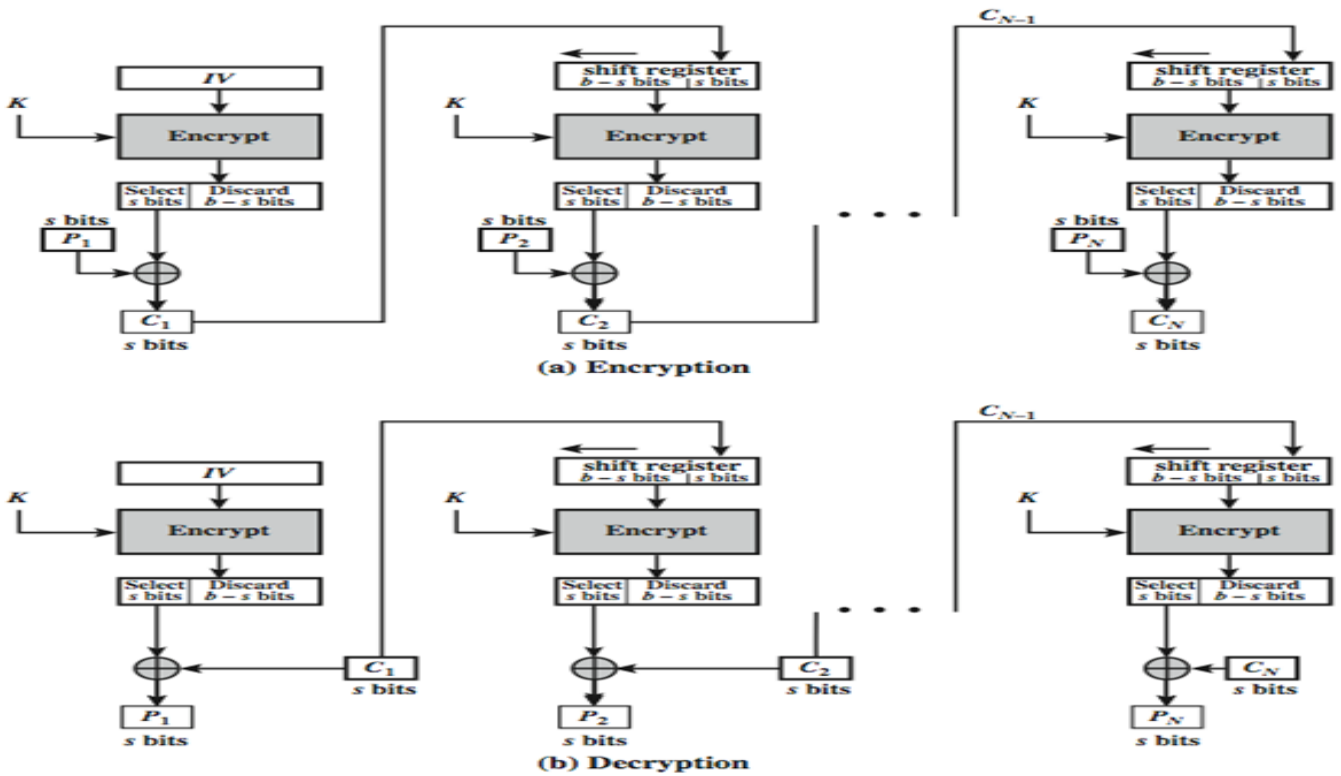
Stream Modes of Operation

- block modes encrypt entire block
- may need to operate on smaller units - real time data
- convert block cipher into stream cipher
  - cipher feedback (CFB) mode
  - output feedback (OFB) mode
  - counter (CTR) mode
  - use block cipher as some form of pseudo-random number generator...

Cipher FeedBack (CFB)

- message is treated as a stream of bits
- added to the output of the block cipher
- result is feed back for next stage (hence name)
- standard allows any number of bits (1,8, 64 or 128 etc) to be feed back
- denoted CFB-1, CFB-8, CFB-64, CFB-128, etc.
- most efficient to use all bits in block (64 or 128)
  $C_i = P_i \oplus E_K(C_{i-1})$
  $C_{-1} = \text{IV}$
- uses: stream data encryption, authentication

CFB


IV
K
Encrypt
Select s bits
Discard b − s bits
s bits
P1
C1
s bits
shift register b − s bits | s bits
P2
C2
CN−1
PN
CN
(a) Encryption
(b) Decryption

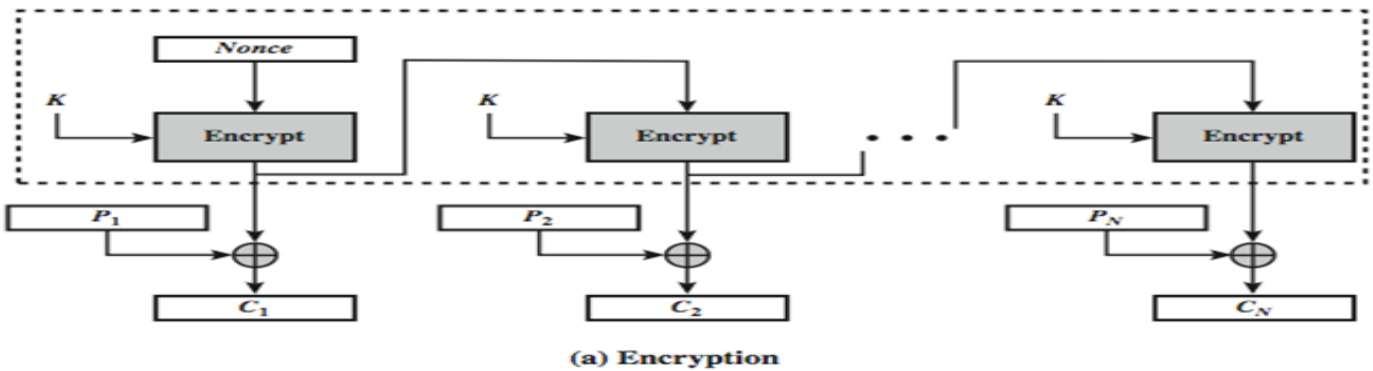
Advantages and Limitations of CFB

- most common stream mode
- appropriate when data arrives in bits/bytes
- limitation is need to stall while do block encryption after every s-bits
- note that the block cipher is used in encryption mode at both ends (XOR)
- errors propagate for several blocks after the error

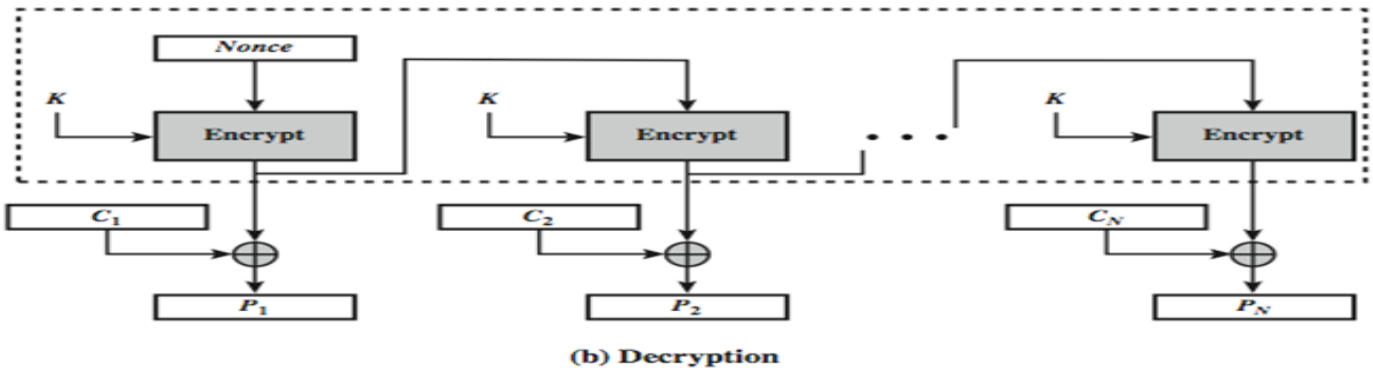
Output FeedBack (OFB)

- message is treated as a stream of bits
- output of cipher is added to message
- output is then feed back (hence name)
  $O_i = E_K(O_{i-1})$
  $C_i = P_i \oplus O_i$
  $O_{-1} = \mathrm{IV}$
- feedback is independent of message
- can be computed in advance
- uses: stream encryption on noisy channels

OFB



(a) Encryption



(b) Decryption

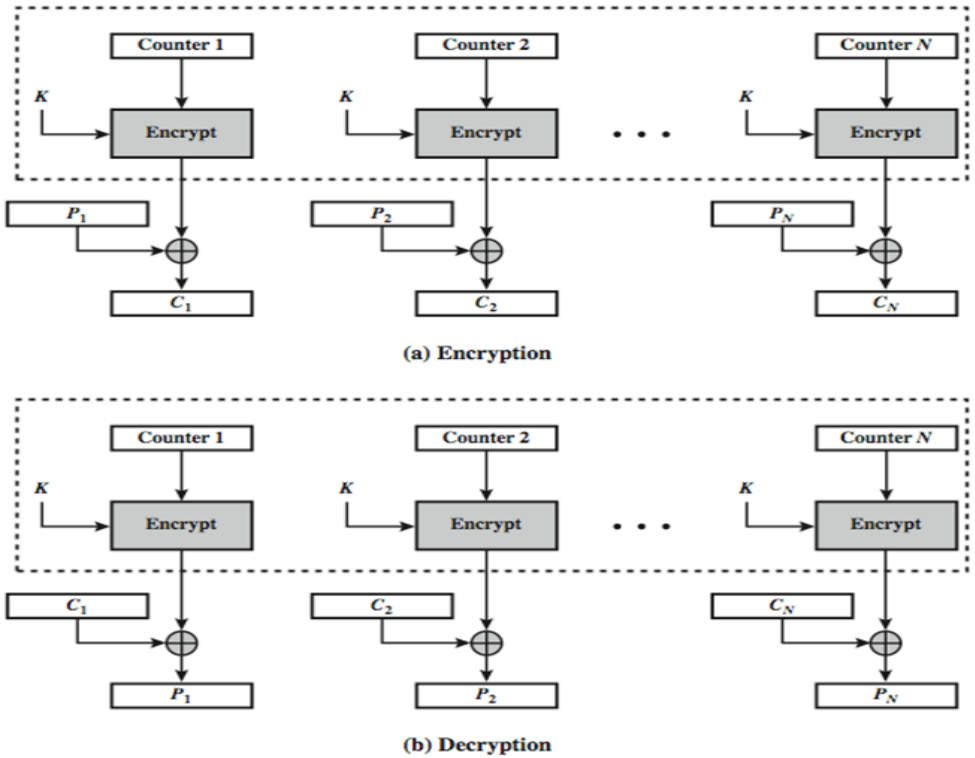
Advantages and Limitations of OFB

- needs an IV which is unique for each use
- if ever reuse attacker can recover outputs
- OTP
- can pre-compute
- bit errors do not propagate
- more vulnerable to message stream modification
- change arbitrary bits by changing ciphertext
- sender & receiver must remain in sync
- only use with full block feedback

Counter (CTR)

- similar to OFB but encrypts counter value rather than any feedback value
  $O_i = E_K(i)$
  $C_i = P_i \oplus O_i$
- must have a different key & counter value for every plaintext block (never reused) again, OTP issue
- uses: high-speed network encryptions

CTR


Counter 1
Counter 2
Counter N
K
Encrypt
P_1
P_2
P_N
C_1
C_2
C_N
(a) Encryption
(b) Decryption

Advantages and Limitations of CTR

- efficiency
- can do parallel encryptions in h/w or s/w
- can preprocess in advance of need
- good for bursty high speed links
- random access to encrypted data blocks
- provable security (good as other modes)
- never have cycle less than 2_b
- but must ensure never reuse key/counter values, otherwise could break (cf OFB)

Summary

- Multiple Encryption & Triple-DES
- Modes of Operation
  ECB, CBC, CFB, OFB, CTR,