Chapter 6

Block Cipher Operation

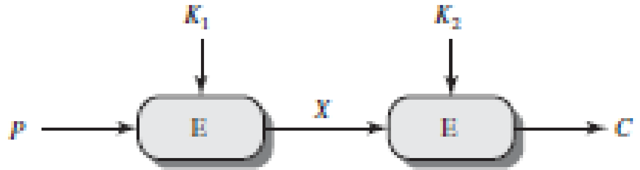
Double DES

- The simplest form of multiple encryption has two encryption stages and two keys.
- Given a plaintext **P** and two encryption keys **(K_1 & K_2)**, ciphertext **C**

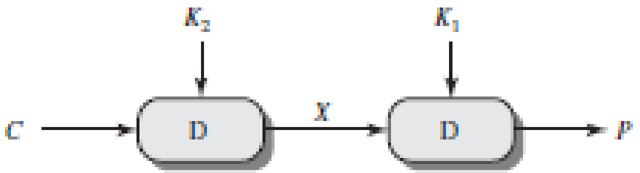
$$C = \mathrm{E}(K_2, \mathrm{E}(K_1, P))$$

$$P = \mathrm{D}(K_1, \mathrm{D}(K_2, C))$$

- For DES, key length 56×2 = 112 bits



Encryption



Decryption

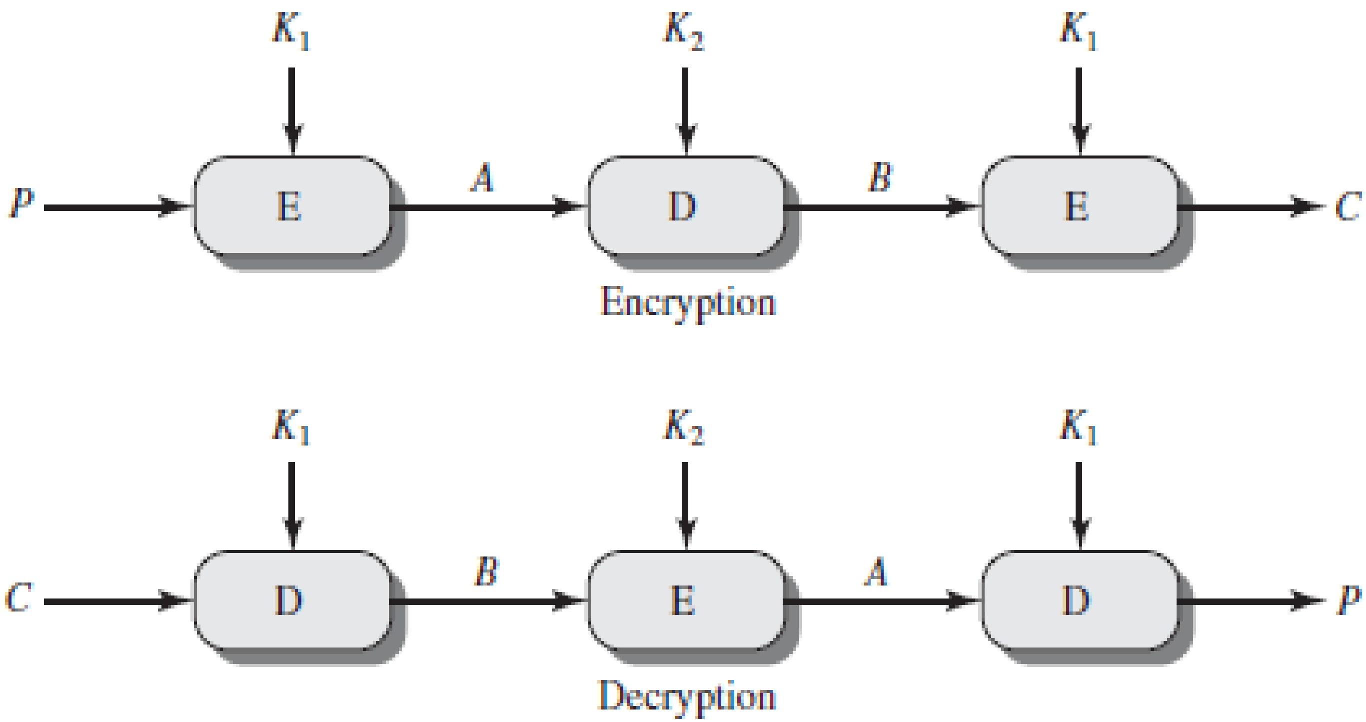
MEET-IN-THE-MIDDLE ATTACK

$$C = E(K_2, E(K_1, P))$$

$$X = E_{K1}(P) = D_{K2}(C)$$

- Encrypt **P** for all $\mathbf{2^{56}}$ possible values of K_1 and store
- Decrypt C using all $\mathbf{2^{56}}$ possible values of $\mathbf{K_2}$ and match X value.
- Total encryption + decryption = $2^{56} \times 2 = 2^{57}$
- On Average, 2^{56} searches
- Reduced from 2^{112} to 2^{56}

Triple-DES with Two-Keys



$$C = \mathrm{E}(K_1, \mathrm{D}(K_2, \mathrm{E}(K_1, P)))$$

$$P = \mathrm{D}(K_1, \mathrm{E}(K_2, \mathrm{D}(K_1, C)))$$

Triple-DES with Two-Keys

- 3 encryptions seem to need 3 distinct keys but can use 2 keys with E-D-E sequence

$$C = E_{K1}(D_{K2}(E_{K1}(P)))$$

$$P = D_{K1}(E_{K2}(D_{K1}(C)))$$

Key length 112 bits

– if $K_1 = K_2$ then can work with single DES

$$C = E(K_1, D(K_1, E(K_1, P))) = E(K_1, P)$$

$$P = D(K_1, E(K_1, D(K_1, C))) = D(K_1, C)$$

Key length 56 bits

Triple-DES with Three-Keys

$$C = E_{K3}(D_{K2}(E_{K1}(P)))$$

Key length = 168 bits

- has been adopted by some Internet applications

Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 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 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-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

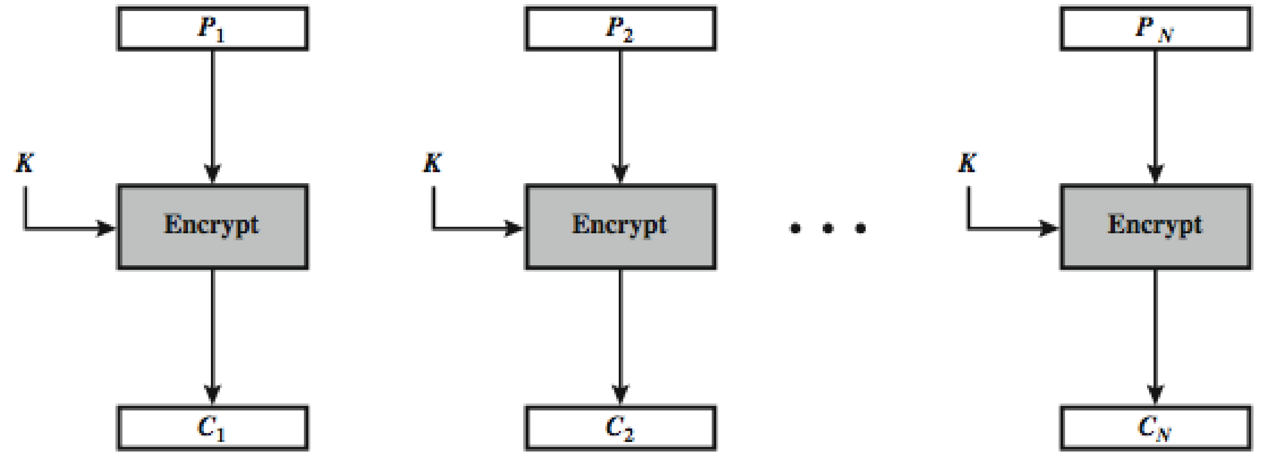
Electronic Codebook Book (ECB)

- message is broken into independent blocks which are encrypted
- each block is a value which is substituted.
- each block is encoded independently of the other blocks

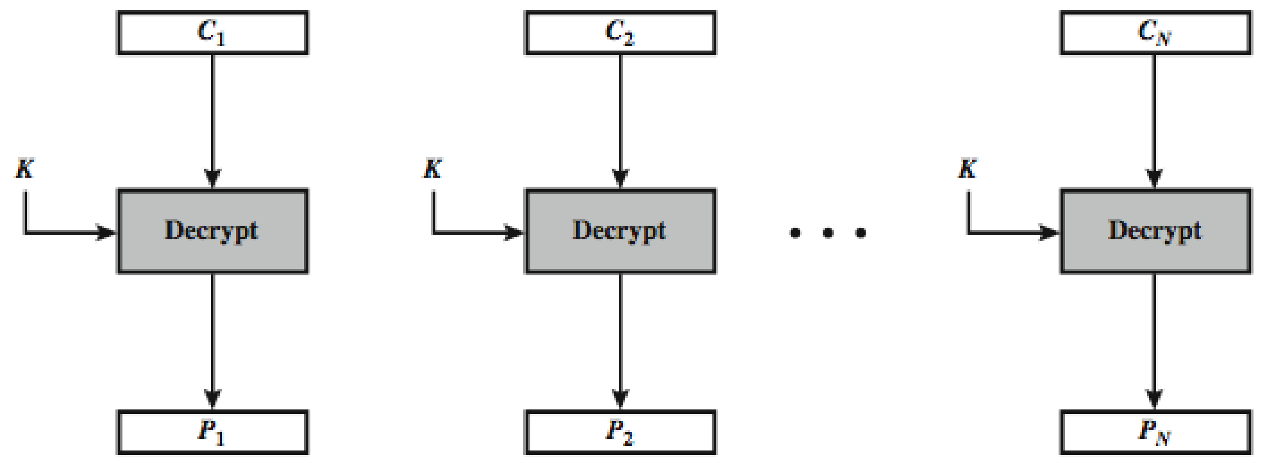
$$C_i = E_K(P_i)$$

- uses: secure transmission of single values

Electronic Codebook Book (ECB)



(a) Encryption



(b) Decryption

ECB	$C_j = E(K, P_j)$	$j = 1, \ldots, N$	$P_j = D(K, C_j)$	$j = 1, \ldots, N$

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
- main use is sending a few blocks of data

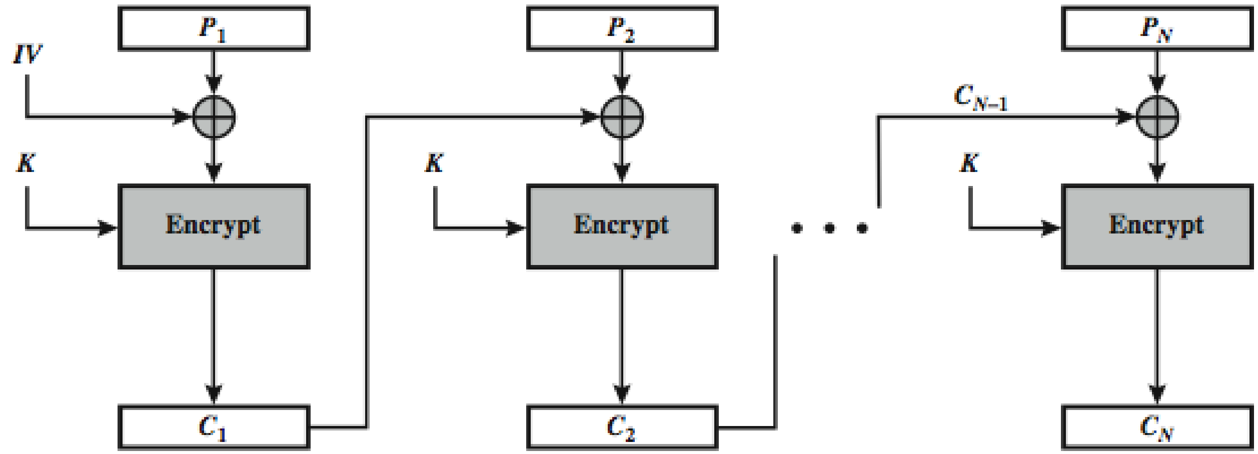
Cipher Block Chaining (CBC)

- message is broken into blocks
- linked together in encryption operation
- XOR current P block and previous C block, so identical P blocks produce different C blocks
- Suitable for long messages.
- Initial Vector (IV) is XORed with first block to start process

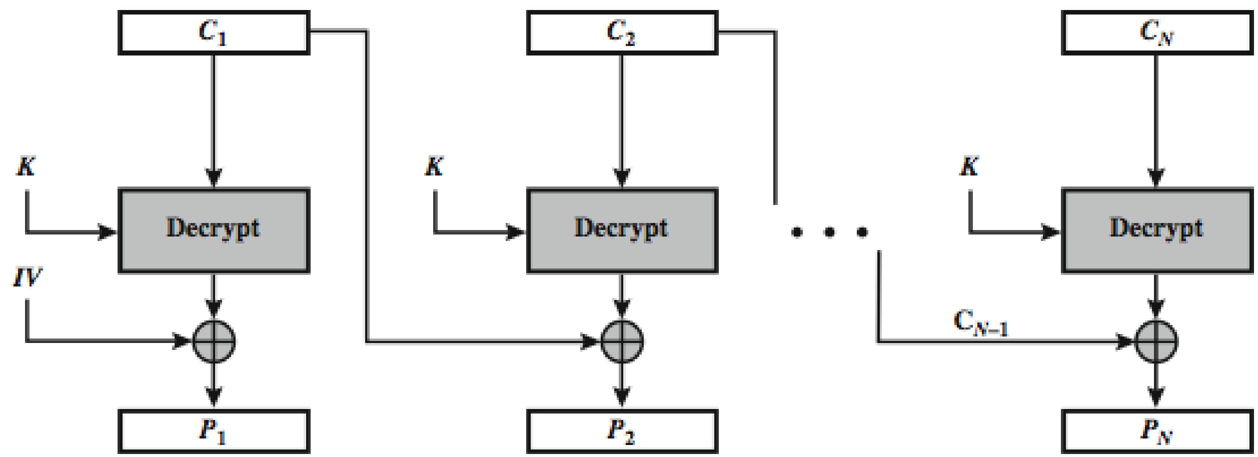
$$C_i = E_K(P_i \text{ XOR } C_{i-1})$$
$$C_{-1} = IV$$

- uses: bulk data encryption, authentication

Cipher Block Chaining (CBC)



(a) Encryption



(b) Decryption

CBC	$C_1 = \mathrm{E}(K, [P_1 \oplus \mathrm{IV}])$ $C_j = \mathrm{E}(K, [P_j \oplus C_{j-1}])\quad j = 2, \ldots, N$	$P_1 = \mathrm{D}(K, C_1) \oplus \mathrm{IV}$ $P_j = \mathrm{D}(K, C_j) \oplus C_{j-1}\quad j = 2, \ldots, N$

Advantages and Limitations of CBC

- 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, and change IV to compensate
  - hence IV must either be a fixed value
  - or must be sent encrypted in ECB mode before rest of message

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

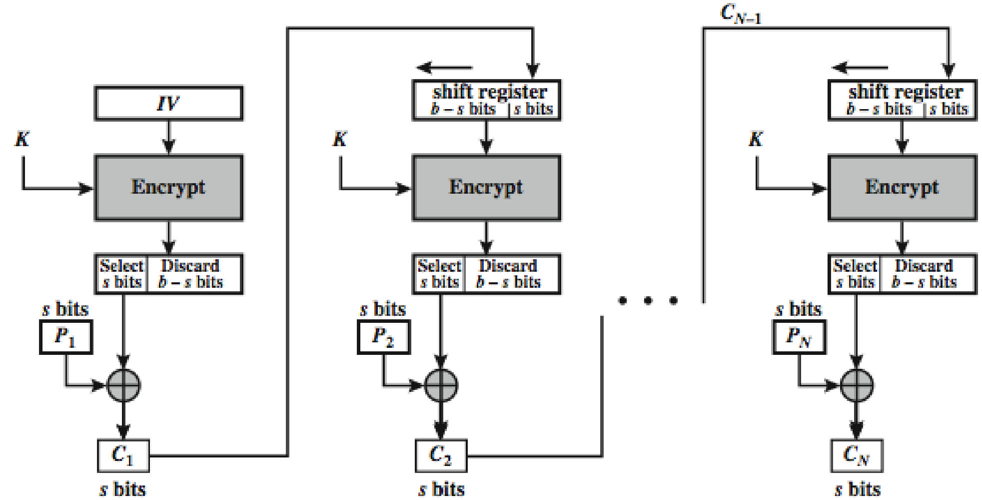
Cipher FeedBack (CFB)

- message is treated as a stream of bits
- added to the output of the block cipher
- result is feed back for next stage.
- standard allows any number of bit (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)

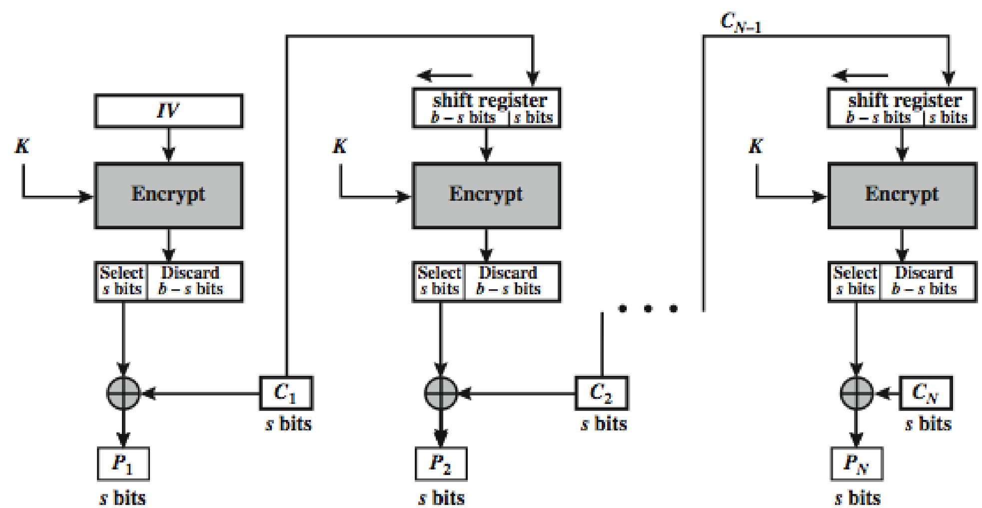
  $C_i = P_i \text{ XOR } E_K(C_{i-1})$

  $C_{-1} = IV$
- uses: stream data encryption, authentication

s-bit Cipher FeedBack (CFB-s)



(a) Encryption



(b) Decryption

CFB	$I_1 = IV$ $I_j = \mathrm{LSB}_{b-s}(I_{j-1}) \parallel C_{j-1} \quad j = 2, \ldots, N$ $O_j = \mathrm{E}(K, I_j) \quad j = 1, \ldots, N$ $C_j = P_j \oplus \mathrm{MSB}_s(O_j) \quad j = 1, \ldots, N$	$I_1 = IV$ $I_j = \mathrm{LSB}_{b-s}(I_{j-1}) \parallel C_{j-1} \quad j = 2, \ldots, N$ $O_j = \mathrm{E}(K, I_j) \quad j = 1, \ldots, N$ $P_j = C_j \oplus \mathrm{MSB}_s(O_j) \quad j = 1, \ldots, N$

Advantages and Limitations of CFB

- appropriate when data arrives in bits/bytes
- limitation is need while do block encryption after every n-bits
- note that the block cipher is used in **encryption** mode at **both** ends
- 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.
- feedback is independent of message
- can be computed in advance

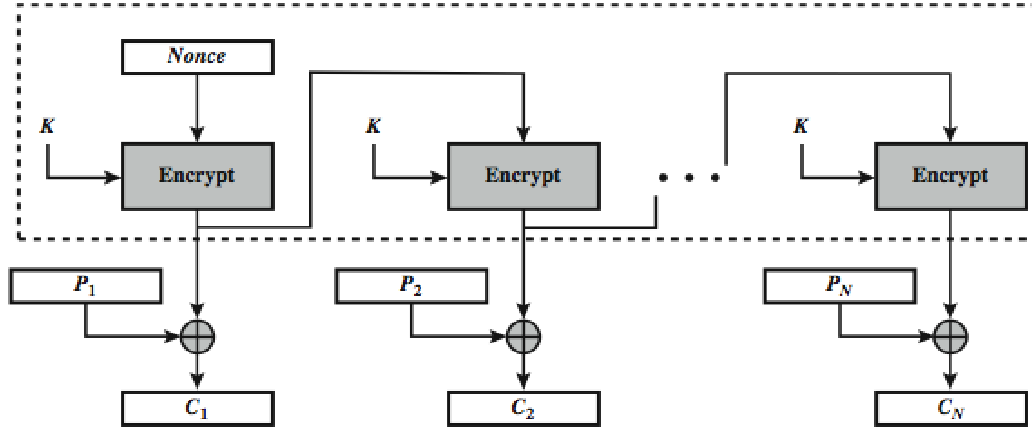
$$O_i = E_K(O_{i-1})$$

$$C_i = P_i \text{ XOR } O_i$$

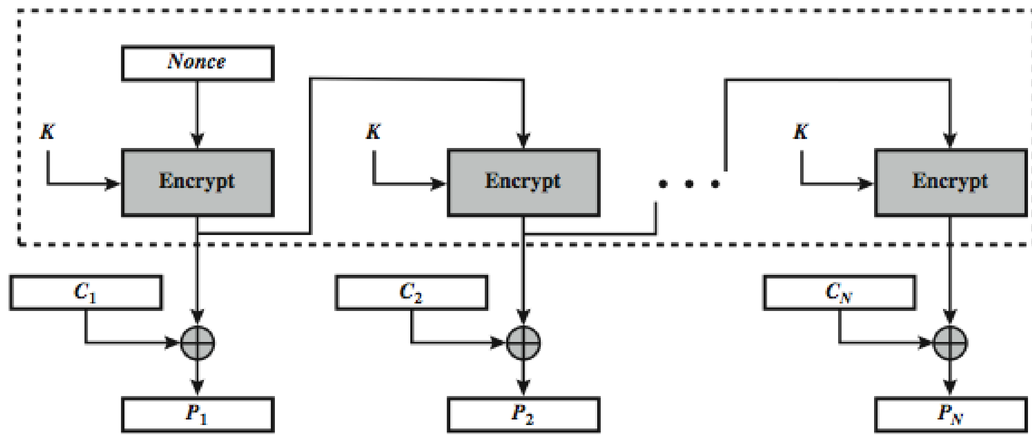
$$O_{-1} = IV$$

- uses: stream encryption on noisy channels

Output FeedBack (OFB)



(a) Encryption



(b) Decryption

OFB	$I_1 = Nonce$ $I_j = O_{j-1} \quad j = 2, \ldots, N$ $O_j = E(K, I_j) \quad j = 1, \ldots, N$ $C_j = P_j \oplus O_j \quad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus MSB_u(O_N)$	$I_1 = Nonce$ $I_j = LSB_{b-s}(I_{j-1}) \parallel C_{j-1} \quad j = 2, \ldots, N$ $O_j = E(K, I_j) \quad j = 1, \ldots, N$ $P_j = C_j \oplus O_j \quad j = 1, \ldots, N-1$ $P_N^* = C_N^* \oplus MSB_u(O_N)$

Advantages and Limitations of OFB

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

Counter (CTR)

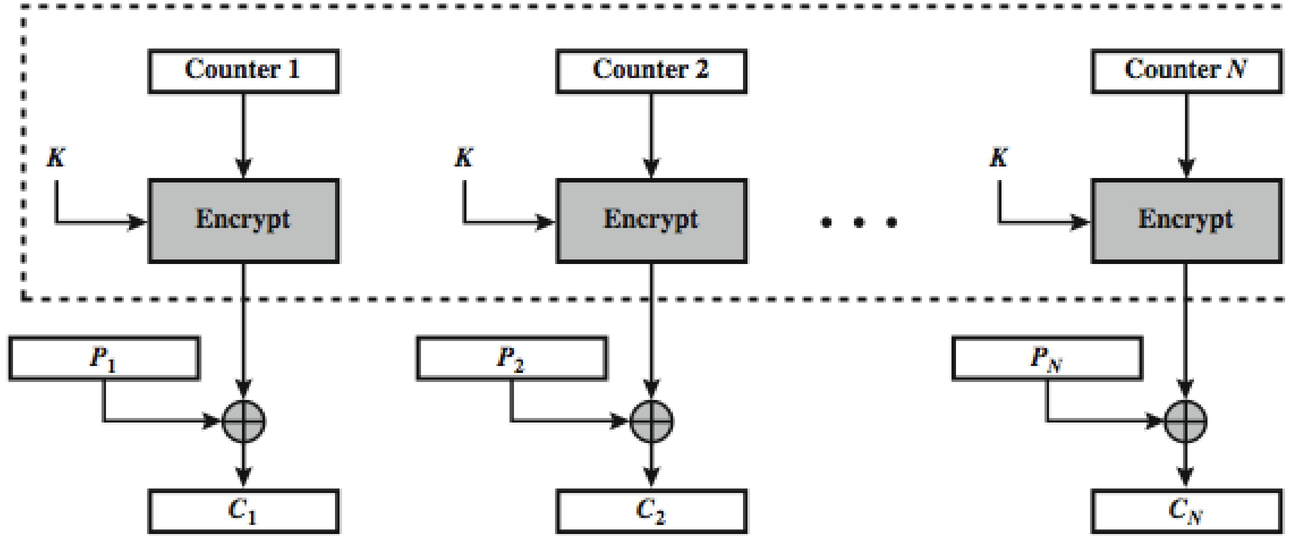
- a “new” mode, though proposed early on similar to OFB but encrypts counter value rather than any feedback value
- must have a different key & counter value for every plaintext block (never reused)

$$O_i = E_K(i)$$

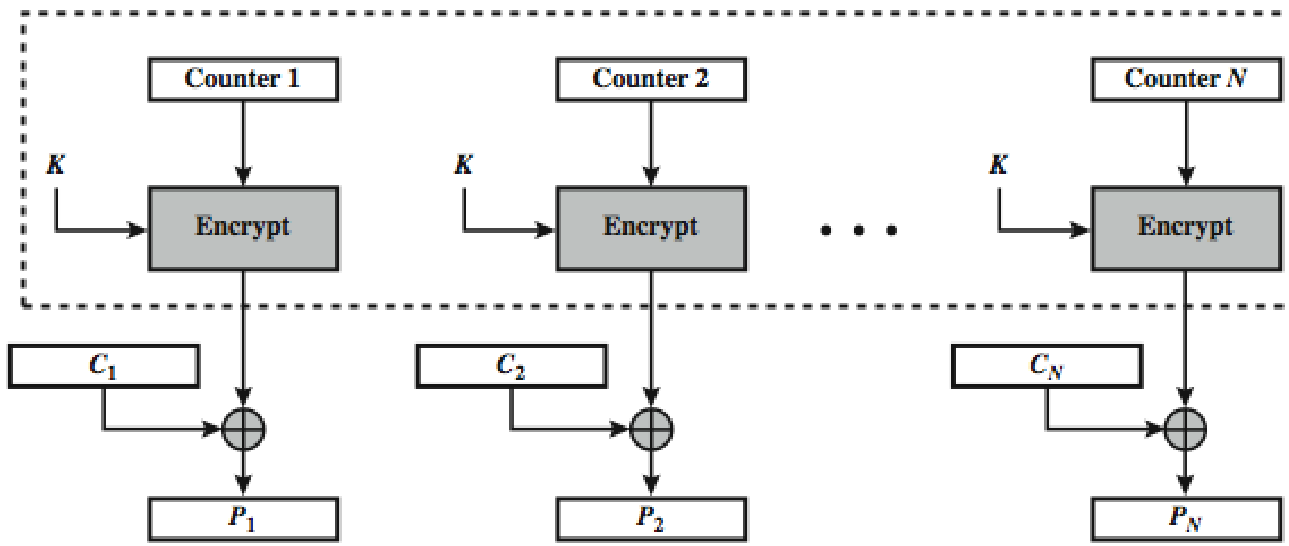
$$C_i = P_i \text{ XOR } O_i$$

- uses: high-speed network encryptions

Counter (CTR)



(a) Encryption

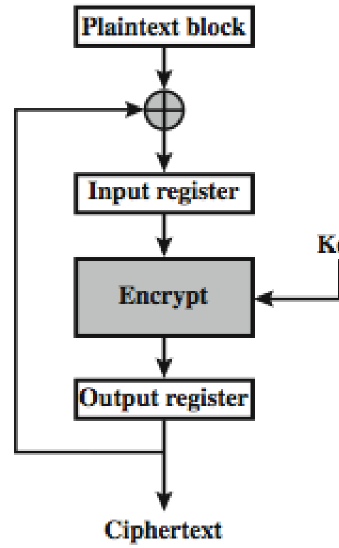


(b) Decryption

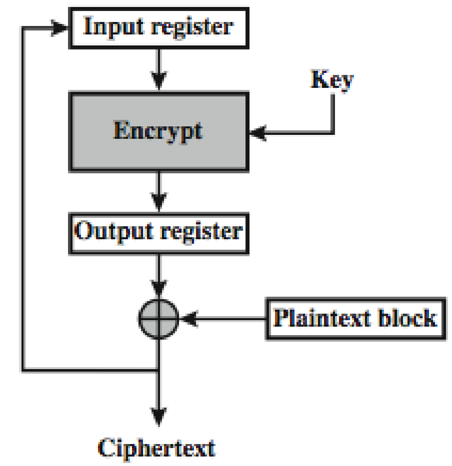
Advantages and Limitations of CTR

- 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)
- but must ensure never reuse key/counter values, otherwise could break (cf OFB)

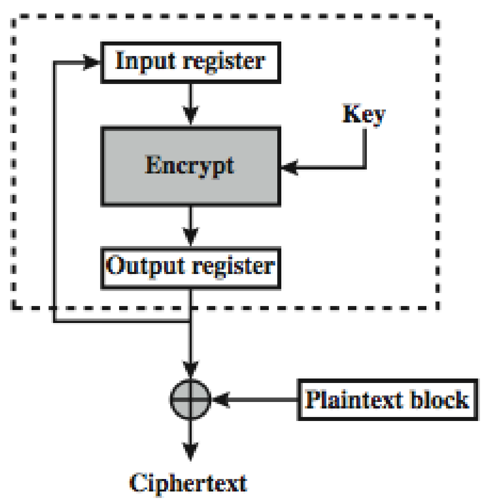
Feedback Characteristics



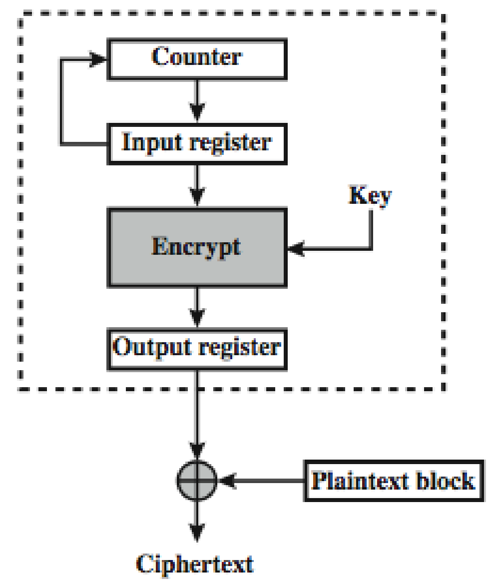
(a) Cipher block chaining (CBC) mode



(b) Cipher feedback (CFB) mode



(c) Output feedback (OFB) mode



(d) Counter (CTR) mode