Lecture 5: Block Cipher Modes of Operation

Stephen Huang

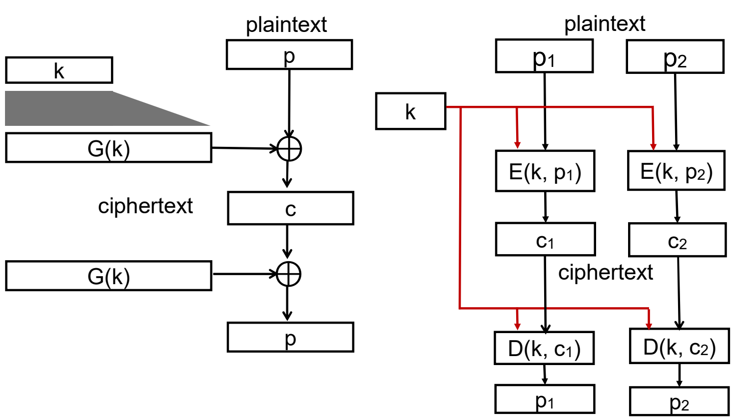
Content

1. Multiple Encryption
2. Block Cipher Modes of Operation: How to use block ciphers in practice.

Encryption Review

Stream ciphers

Block ciphers

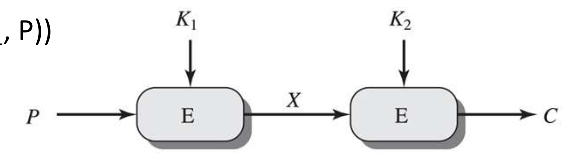


1. Multiple Encryption

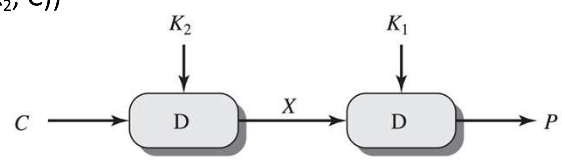
- Why we do not like DES (anymore):
  - Key size is only 56 bits → 2^{56} steps brute-force attacks are feasible.
- Why we still like DES:
  - Relatively secure against cryptanalytic attacks (best attack: linear cryptanalysis in 2^{43} steps).
  - Thoroughly studied and widely supported.
- Multiple encryption
  - Use the same encryption algorithm multiple times, each time with a different key.
  - Widely used with DES, but the principle can be applied to any block cipher.

Double DES

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



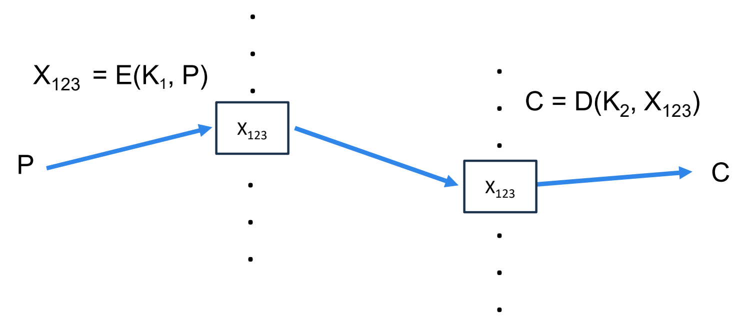
$P = D(K_1, D(K_2, C))$



key size = 2 × 56 = 112 bits

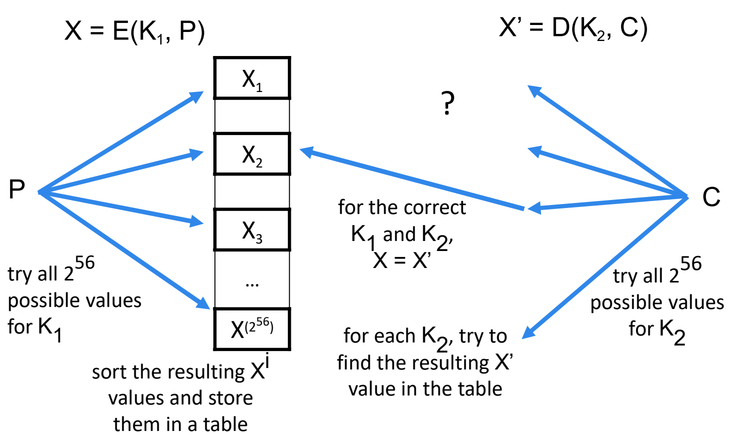
Double DES

Known-plaintext attack: suppose that the attacker has a pair P, C

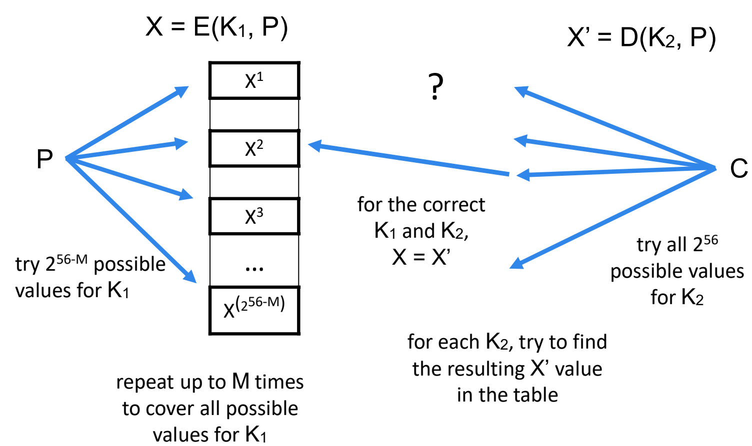


Meet-in-the-Middle Attack

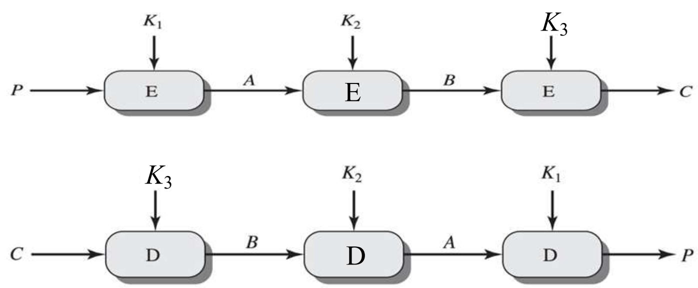
Known-plaintext attack: suppose that the attacker has a pair P, C



MitM Attack Requirements

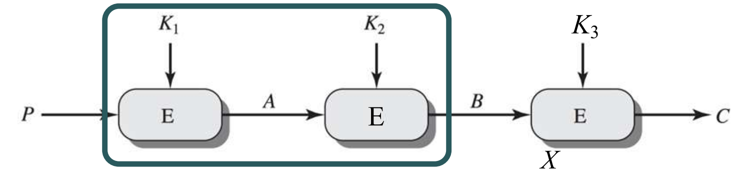


Triple DES (3DES)



Triple DES (3DES)

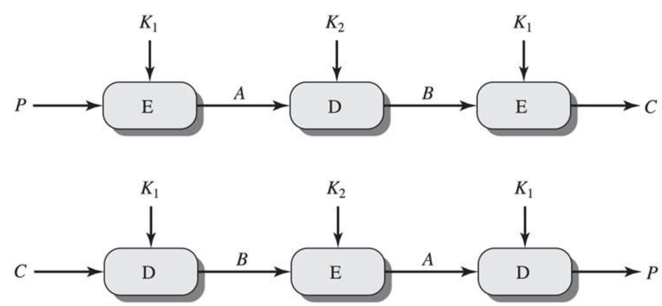
- Three keys (3 × 56 = 168-bit key)
  - more complex meet-in-the-middle attack → effective security is only 112 bits.
  - 3DES can be viewed as a combination of two ciphers: one with a 56-bit key and one with a 112-bit key.



encryption with 112-bit key (K_1 and K_2)

encryption with 56-bit key (K_3)

Triple DES with Two Keys



Triple DES

- Two keys (2 × 56 = 112-bit key)
  - Prevents the simple meet-in-the-middle attack presented earlier
  - However, there are other known-plaintext attacks → According to NIST, this approach provides around 80 bits of security
- EDE (Encryption-Decryption-Encryption) configuration
  - if K1 = K2, then 3DES is equivalent to DES → Compatibility with older systems
- Unfortunately, 3DES is very slow and has a small block size.

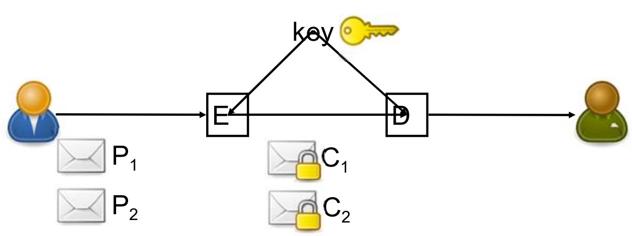
2. Block Cipher Modes of Operation

- Key Reuse
- Block Cipher Modes of Operation
  a. Electronic Code Book (ECB)*
  b. Cipher Block Chaining (CBC)*
  c. Using Block Ciphers as Stream Ciphers
  d. Output Feedback (OFB)*
  e. Cipher Feedback (CFB)*
  f. Counter (CTR)*

Key Reuse

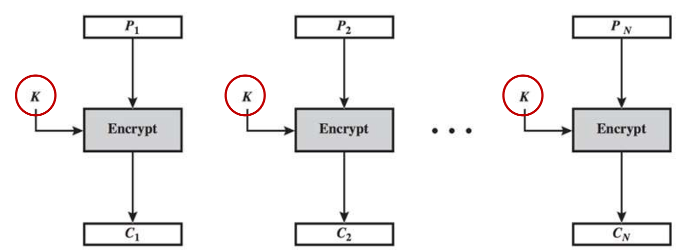
- We may have to use the same key to encrypt multiple blocks.
  – Multiple plaintexts (e.g., sending multiple messages over an insecure channel).
  – Long plaintext → break up into fixed-size blocks
    P = "The quick brown fox jumps"
    P1 = "The quick bro"   P2 = "wn fox jumps"
- Reminder: key reuse issue with stream ciphers (and one-time pad)
  – same key → same pseudorandom sequence
    → C1 ⊕ C2 = P1 ⊕ P2

Key Reuse



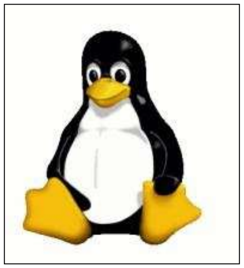
Encrypting Multiple Blocks

- Simplest approach: encrypt each block independently
  – Secure encryption is indistinguishable from random permutation to the attacker
    → if $P_1 \neq P_2$, then C_1 and C_2 look like unrelated random blocks
  – Encryption is invertible
    → if $P_1 = P_2$, then $C_1 = C_2$

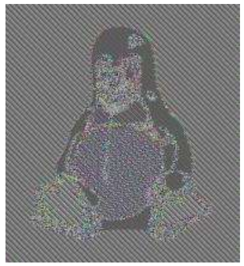


Repeating Blocks

- In practice, many protocols/file formats have predefined headers and elements → repeating blocks.



Plaintext (bitmap)



Ciphertext

Block Cipher Modes of Operation

- Mode of operation: a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application (e.g., applying a block cipher to a sequence of blocks)
- Five standard modes of operation (NIST Special Publication 800-38A)
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Output Feedback (OFB)
  - Cipher Feedback (CFB)
  - Counter Mode (CTR)
- These modes can be used with any block cipher (DES, AES)
- Criteria: security, efficiency, integrity (error recovery/ propagation)

a. Electronic Code Book (ECB)

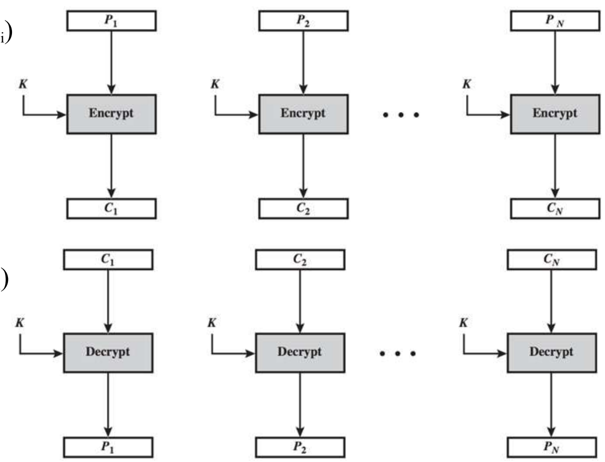
- The simplest mode is the electronic codebook (ECB) mode, in which plaintext is handled one block at a time, and each plaintext block is encrypted using the same key.
- The term codebook is used because, for a given key, there is a unique ciphertext for every b-bit block of plaintext.
- For a message longer than b bits, the procedure is simply to break the message into b-bit blocks, padding the last block if necessary.

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

Electronic Code Book (ECB)

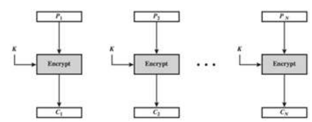
$C_i = E(K, P_i)$

$P_i = D(K, C_i)$



Electronic Code Book (ECB)

- Identical plaintext blocks result in identical ciphertext blocks
- Blocks can be encrypted or decrypted in parallel
  - We can start decryption with any block
- Bit error in the ciphertext
  - Corresponding plaintext block becomes random
- Attacker can rearrange or remove blocks from the ciphertext
  - Additional integrity protection is necessary



ECB: Reordering Blocks

Plaintext

Transfer one	million USD to	John Smith's	account from	John Doe's	account.

Ciphertext

dgyACJVKcERNl	z9iIcfkeBEYE2	sp1uELybLi3wm	fq6aSDNIa6wn6	5YRnb75iDRSFx	wFR0yVk1UrIx0

Modified ciphertext

dgyACJVKcERNl	z9iIcfkeBEYE2	5YRnb75iDRSFx	fq6aSDNIa6wn6	sp1uELybLi3wm	wFR0yVk1UrIx0

Modified plaintext

Transfer one	million USD to	John Doe's	account from	John Smith's	account.

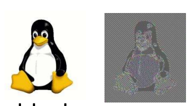
ECB Summary

Advantages

- blocks can be encrypted or decrypted in parallel (i.e., multiple blocks can be encrypted or decrypted at the same time).

Disadvantages

- Identical plaintext blocks result in identical ciphertext blocks.
- The attacker can rearrange or remove blocks from the ciphertext, and the receiver won't know it.



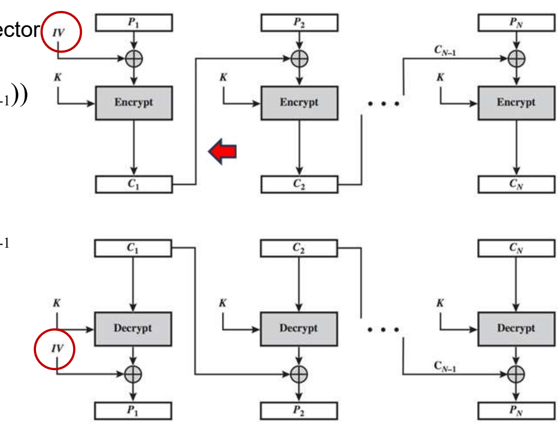
Application: Secure transmission of a single block.

b. Cipher Block Chaining (CBC)

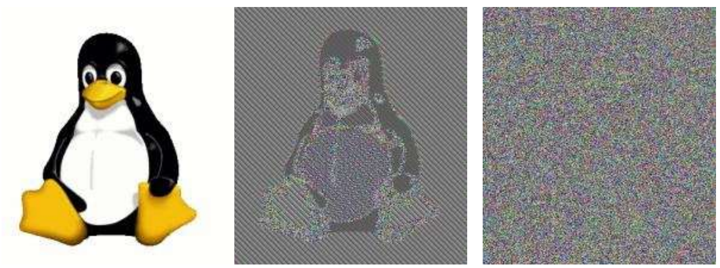
initialization vector

$C_i = E(K, (P_i \oplus C_{i-1}))$

$P_i = D(K, C_i) \oplus C_{i-1}$



CBC: Repetitive Plaintext



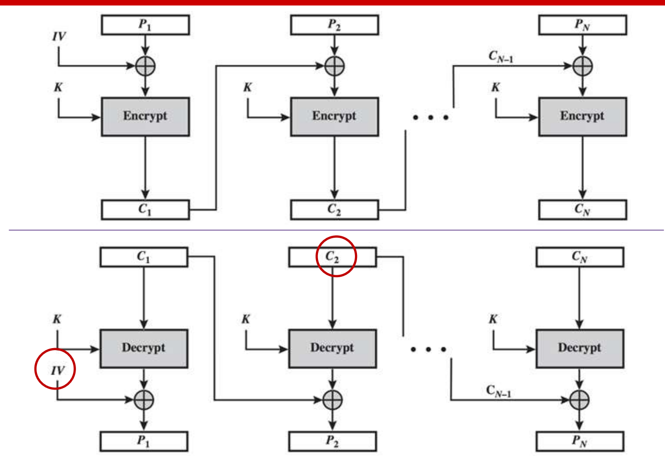
Plaintext ECB CBC

Ciphertext

CBC Details

- Blocks can be decrypted in parallel but not encrypted. Why?
- A bit-error in the ciphertext causes the corresponding plaintext block to become random, and a bit-error in the next plaintext block.
  - The attacker may flip some bits in a plaintext block (but the following block becomes random)
- Initialization vector (IV) does not have to be secret but must be protected (unpredictable by a third party).
  - If the attacker can change some bits in the IV, then the corresponding bits in the first plaintext block change.
- The chaining operation makes the ciphertext blocks dependent on the current and all preceding plaintext blocks, and therefore, blocks can not be rearranged.

CBC

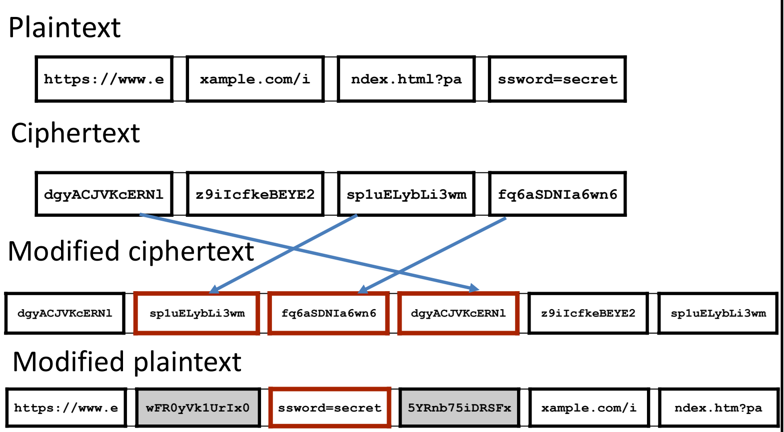


Cutting & Pasting CBC Messages

- Consider the encrypted message

  $IV, C_1, C_2, C_3, C_4, C_5$.
- The shortened message IV, C_1, C_2, C_3, C_4 appears valid.
- The truncated message C_2, C_3, C_4, C_5 is valid: C_2 acts as the IV. It decrypts to P_3, P_4, P_5.
- Even C_2, C_3, C_4 is valid, and will decrypt properly to P_3, P_4.
- Any subset of a CBC message will decrypt cleanly.
- If we snip out blocks, leaving IV, C_1, C_4, C_5, we only corrupt one block of plaintext.
- Conclusion: If you want message integrity, you must do it yourself.

Cutting & Pasting CBC Messages



CBC: Summary

- Advantages:
  - Hides patterns in the plaintext.
  - Blocks can be decrypted in parallel.
- Disadvantages:
  - Blocks cannot be encrypted in parallel.
  - The attacker might be able to rearrange or remove blocks from the ciphertext.
  - IV needs integrity protection.
  - The attacker might be able to tamper with the bits of the plaintext.
- Application: general-purpose block-oriented transmission.
- Probably the most popular mode of operation for general-purpose block-oriented transmission.

c. Block Ciphers as Stream Ciphers

- Short plaintext (*e.g.*, one bit)
  - If we use the previous two modes (ECB or CBC), we need to send an entire block (64 bits for DES and 128 for AES)
  - With stream ciphers, the ciphertext is only as long as the plaintext (*e.g.*, one bit)
- Converting a block cipher into a stream cipher
  - Output Feedback (OFB)
  - Cipher Feedback (CFB)
  - Counter Mode (CTR)
- Stream ciphers always need integrity protection to detect tampering.

Stream Ciphers: Changing Bits

Original Plaintext	Y	E	S
Binart Representation	01011001	01000101	01010011
Pseudorandom Seq.	11010010	00100000	11110101
Original Ciphertext	10001011	01100101	10100110
Modified Ciphertext	10011100	01101111	11010100
Pseudorandom Seq.	11010010	00100000	11110101
XOR	01011001	01001111	00100001
Modified Plaintext	N	O	!

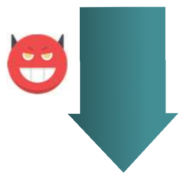
Stream Ciphers: Changing Bits

Plaintext

`Transfer one million dollars to Mr. John Smith's account.`

Ciphertext

`11DE8aAs7gzUovteKIy6G7yttaacP5pFcGPW3m54Nr4Hepdl7kAjr4kfs`



$\oplus$ ("**Smith's**" $\oplus$ "**Doe's **")

Modified Ciphertext

`11DE8aAs7gzUovteKIy6G7yttaacP5pFcGPW3m54N`**ypj9xhJ**`7kAjr4kfs`

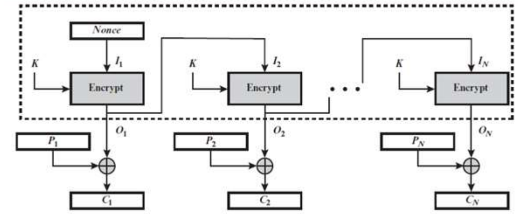
Modified Plaintext

`Transfer one million dollars to Mr. John Doe's   account.`

d. Output Feedback (OFB)

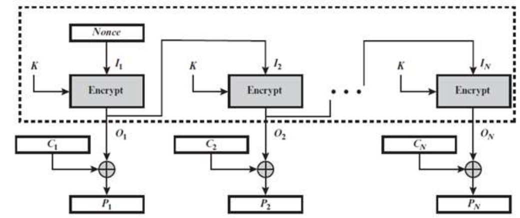
$O_i = E(K, O_{i-1})$

$C_i = P_i \oplus O_i$



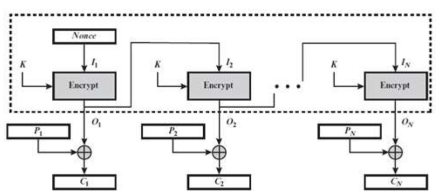
$O_i = E(K, O_{i-1})$

$P_i = C_i \oplus O_i$



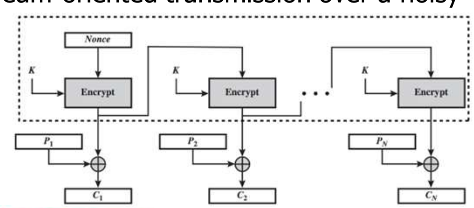
Output Feedback

- Blocks can be neither encrypted nor decrypted in parallel. However, the sequence can be pre-computed.
- No "seeking" to an arbitrary position in the sequence.
- Bit error in the ciphertext → Bit error in the corresponding plaintext block.
  - The attacker can flip bits in plaintext by flipping the corresponding bits in the ciphertext (without introducing any unwanted changes).



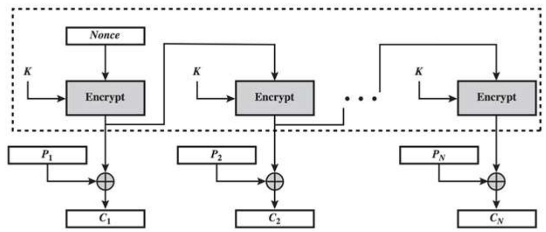
Output Feedback Summary

- Advantages
  - Bit errors do not propagate.
  - Pre-computation is possible.
- Disadvantages
  - Blocks cannot be encrypted or decrypted in parallel (unless the sequence is precomputed).
  - An attacker can tamper with the bits of the plaintext.
- Application: stream-oriented transmission over a noisy channel.

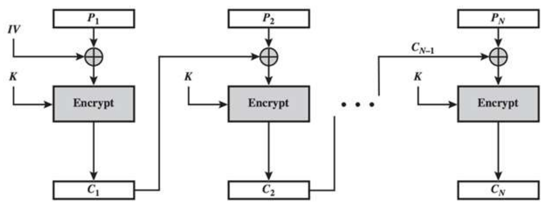


OFB vs. CBC

OFB

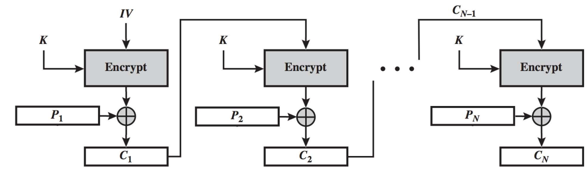


CBC

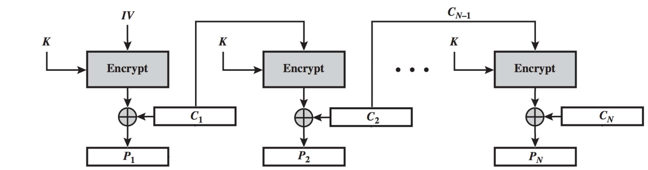


e. *Simplified* Cipher Feedback (CFB)

$C_i = P_i \oplus E(K, C_{i-1})$



$P_i = E(K, C_{i-1}) \oplus C_i$



Cipher Feedback Details

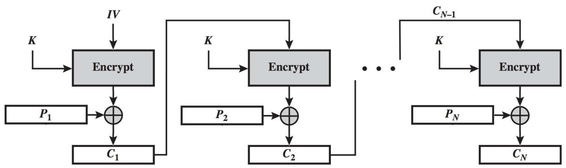
- Blocks can be decrypted in parallel but cannot be encrypted in parallel
- Bit error in the ciphertext implies bit error in the corresponding plaintext block; the next plaintext block becomes random.
- The attacker may flip some bits in a plaintext block (but the next block becomes random)
- Self-synchronizing: decryption requires only the value of the previous ciphertext block, not its position in the ciphertext.

Cipher Feedback Summary

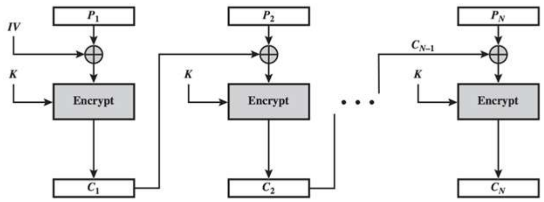
- Advantages
  - Blocks can be decrypted in parallel.
  - Self-synchronizing stream cipher.
- Disadvantages
  - Blocks cannot be encrypted in parallel.
  - An attacker might be able to tamper with the bits of the plaintext.
  - An attacker might be able to rearrange or remove blocks.
- Application: general-purpose stream-oriented transmission.

CFB vs. CBC

CFB Simplified
$C_i = P_i \oplus E(K, C_{i-1})$



CBC
$C_i = E(K, (P_i \oplus C_{i-1}))$

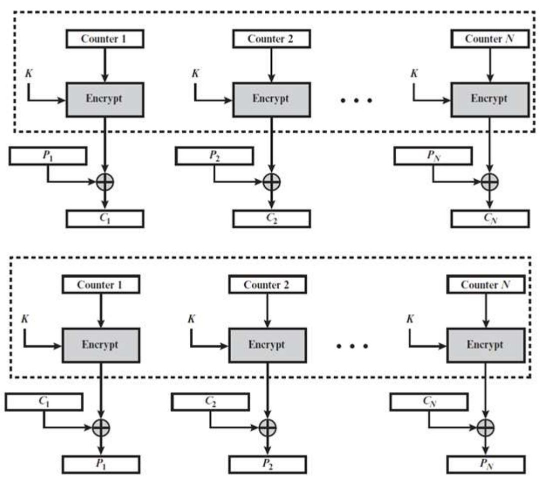


f. Counter (CTR) Mode

- A counter equal to the plaintext block size is used.
- The only requirement is that each encrypted plaintext block's counter value must differ.
- Typically, the counter is initialized to some value and then incremented by 1 for each subsequent block (modulo 2^b, where b is the block size).
- There is no chaining.
- T_j is the counter for the j-th step.

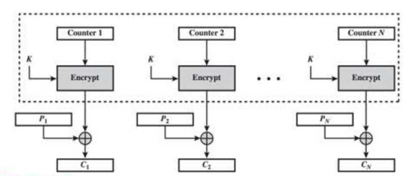
CTR	$C_j = P_j \oplus E(K, T_j) \quad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus MSB_u[E(K, T_N)]$	$P_j = C_j \oplus E(K, T_j) \quad j = 1, \ldots, N-1$ $P_N^* = C_N^* \oplus MSB_u[E(K, T_N)]$

Counter Mode



CTR Detail

- Counter value must be increased after each block, Otherwise, we run into the key-reuse problem for stream ciphers
- Blocks can be both encrypted and decrypted in parallel. Further, the sequence can be precomputed.
- A bit error in the ciphertext implies a bit error in the corresponding plaintext block.
  - The attacker can flip bits in plaintext by flipping the corresponding bits in the ciphertext (without introducing any unwanted changes)



Counter Mode Summary

- Advantages
  - Blocks can be encrypted and decrypted in parallel
  - Bit errors do not propagate
  - Pre-computation is possible
- Disadvantages
  - An attacker can tamper with the bits of the plaintext
- Application: general-purpose transmission

Summary of Standard BCM

- Block-oriented
  - Electronic Code Book (ECB): simplest, used only for transmitting a single block
  - Cipher Block Chaining (CBC): commonly used
- Stream-oriented
  - Output Feedback (OFB): no random access
  - Cipher Feedback (CFB): self-synchronizing stream cipher
  - Counter (CTR): very efficient, very commonly used
- None of these modes provide full integrity protection
  - Authenticated encryption modes: providing confidentiality and integrity protection simultaneously

Next Topics

- Block Cipher Modes of Operation
- Public-Key Encryption
- Hash Functions