Block Cipher Modes of Operation
(CS-452)

Section 6 Block Cipher Modes of Operation

Block Cipher Modes of Operation

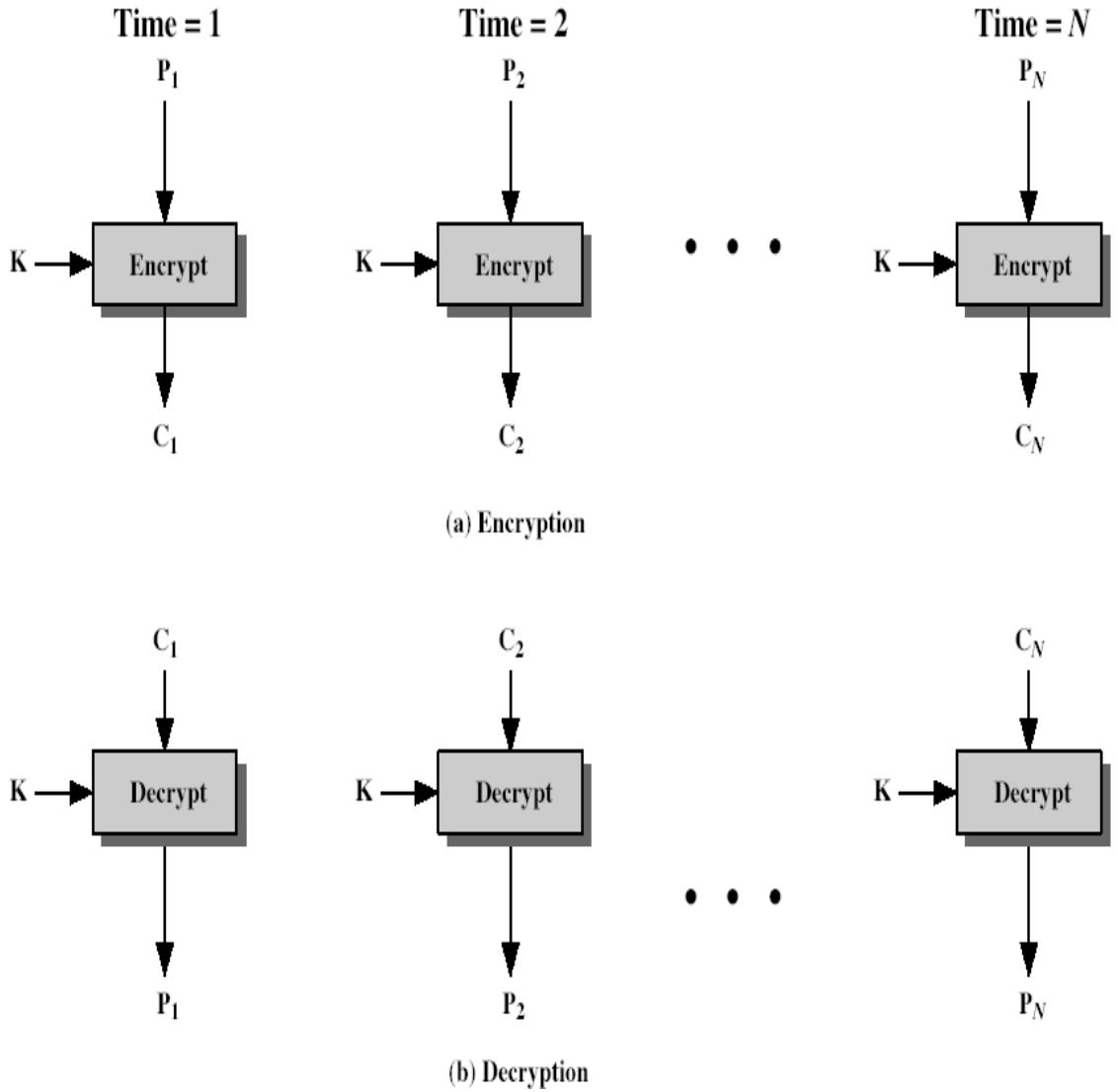
- An n-bit block cipher encrypts plaintext n-bits at a time.
- Plaintexts longer than n bits are split into multiple blocks.
- How should the blocks from the same plaintext be processed?
  - Has implications on security, implementation complexity, etc.
- Block cipher mode of operation: an algorithm that uses block cipher to encrypt multiple blocks of the plaintext in a way that delivers a particular security service.
  - Example: confidentiality and authenticity.

Block Cipher Modes of Operation: Modes

- NIST Special Publication 800-38A defines five modes of block cipher operation:
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)

Electronic Codebook Mode (ECB)

- The message is divided into blocks.
- Plaintext is handled one block at a time and each block is encrypted using the same key.

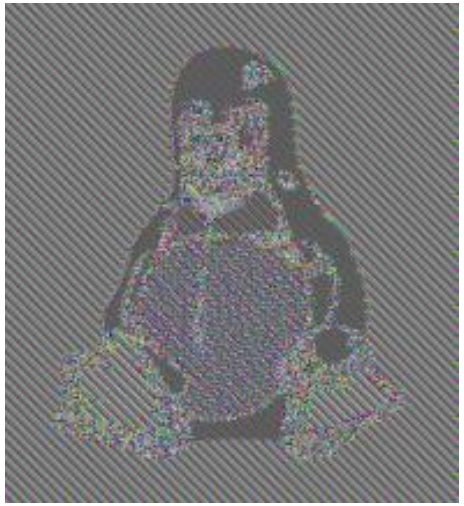


Advantages and Limitations of ECB

- Each block is encrypted independently of the other blocks
- Ideal for a short amount of data, e.g. transmit a DES key securely.
- For lengthy mesg, the ECB mode may not be secure.
  - The same n-bit block of plaintext, if it appears more than once in the mesg., always produces the same ciphertext - does not hide data patterns well.

Example: Disadvantage of ECB

- A pixel-map version of the image on the left was encrypted with ECB mode and with other modes.

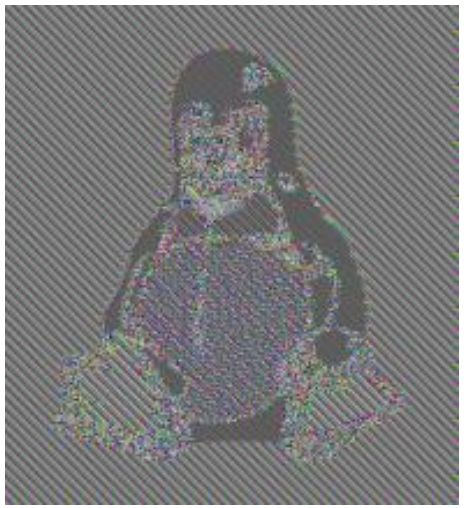


Encrypted using ECB mode

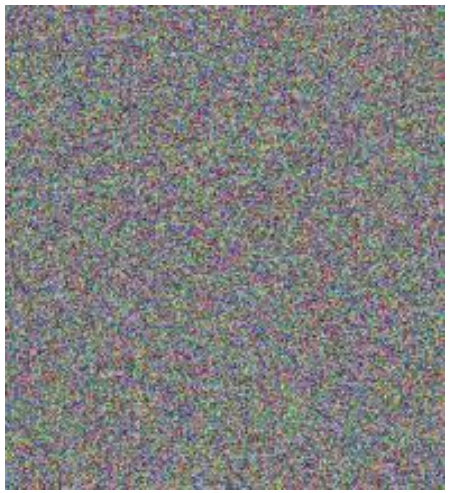
Example: Disadvantage of ECB

- A pixel-map version of the image on the left was encrypted with ECB mode and with other modes.

Original



Encrypted using ECB mode



Encrypted using other modes

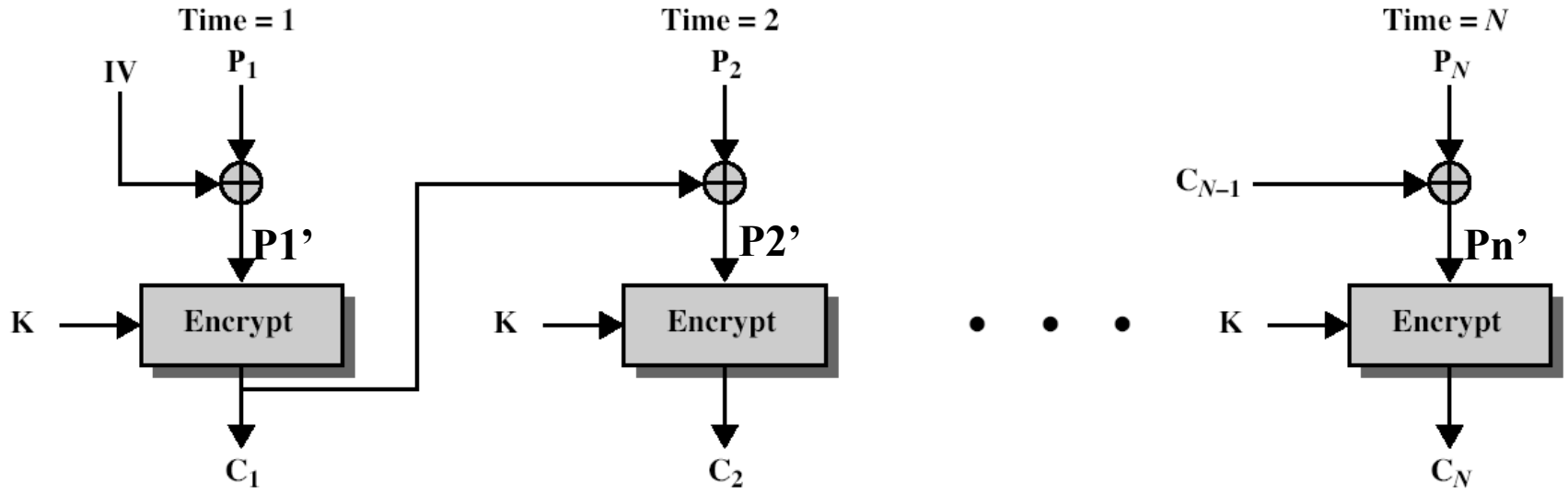
Advantages and Limitations of ECB

- Weakness is due to the encrypted message blocks being independent
  - Would like a technique in which the same plaintext block, if repeated, produces different ciphertext block.

Cipher Block Chaining (CBC)

- The input to the encryption algorithm is the XOR (⊕) of the current plaintext block and the preceding ciphertext block.
- Each ciphertext block is dependent on all plaintext blocks processed up to that point.

  $C_j = E(K,[C_{j-1} \oplus P_j]), C_0 = IV$

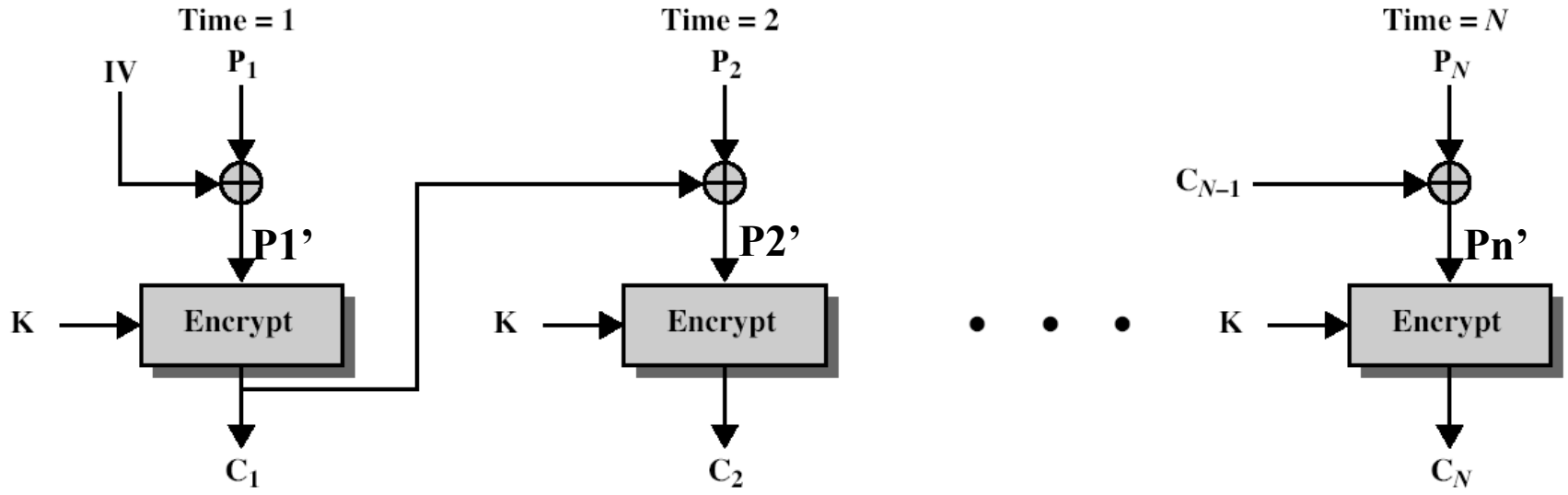


(a) Encryption

Cipher Block Chaining (CBC)

- The input to the encryption algorithm is the XOR (⊕) of the current plaintext block and the preceding ciphertext block. ($A \oplus A = 0, 0 \oplus A = A$)
- Each ciphertext block is dependent on all plaintext blocks processed up to that point.

  $C_j = E(K,[C_{j-1} \oplus P_j]), C_0 = IV$

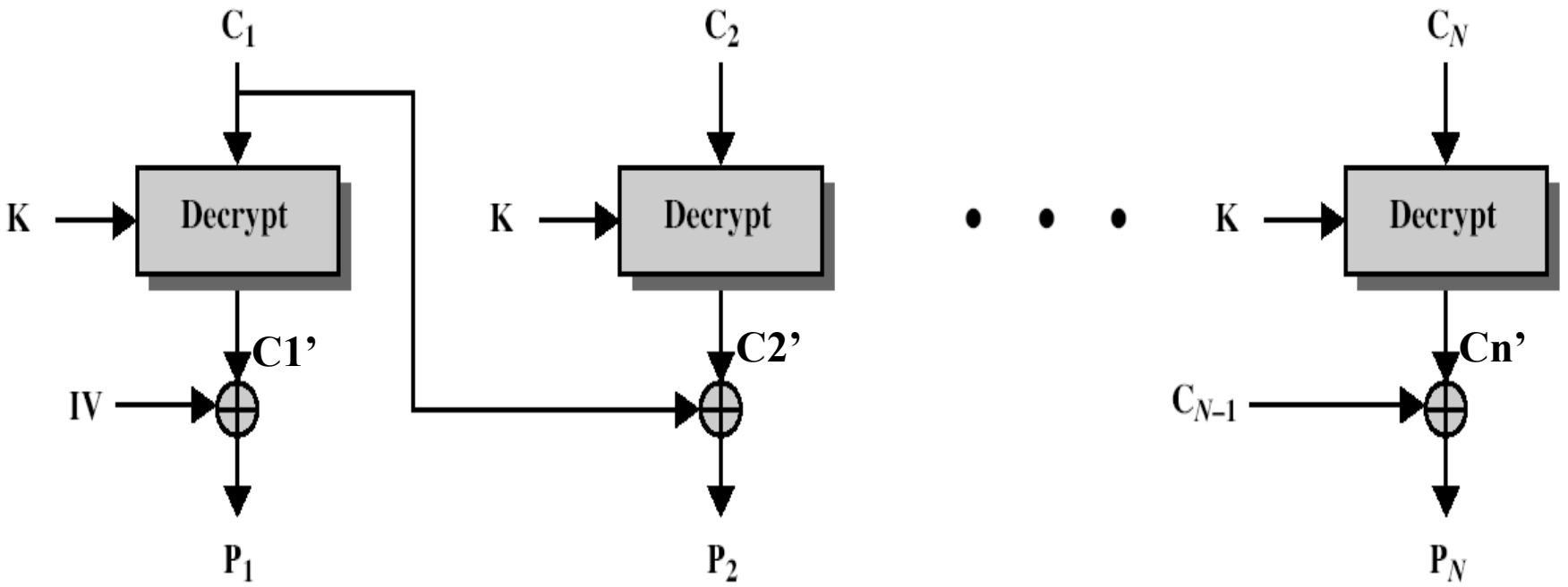


(a) Encryption

Cipher Block Chaining (CBC)

- For decryption, each cipher block is passed through the decryption alg.. The result is XORed with the preceding ciphertext block to produce the plaintext.

  $P_j = C_{j-1} \oplus D(K,C_j)$, $C_0 = IV$



(b) Decryption

Cipher Block Chaining (CBC)

- How to prove that the decryption process is correct?

  Encryption: $C_j = E(K,[C_{j-1} \oplus P_j])$, $C_0 = IV$

  Decryption: $P_j = C_{j-1} \oplus D(K,C_j)$, $C_0 = IV$

Cipher Block Chaining (CBC)

- How to prove that the decryption process is correct?

Encryption: $C_j = E(K,[C_{j-1} \oplus P_j]), C_0 = IV$

Decryption: $P_j = C_{j-1} \oplus D(K,C_j), C_0 = IV$

Proof:

$$A \oplus A = 0$$

$$0 \oplus A = A$$

$$\begin{aligned} P_j &= C_{j-1} \oplus D(K,C_j) \\ &= C_{j-1} \oplus D(K, E(K,[C_{j-1} \oplus P_j])) \\ &= C_{j-1} \oplus C_{j-1} \oplus P_j \\ &= 0 \oplus P_j \\ &= P_j \end{aligned}$$

Message Padding

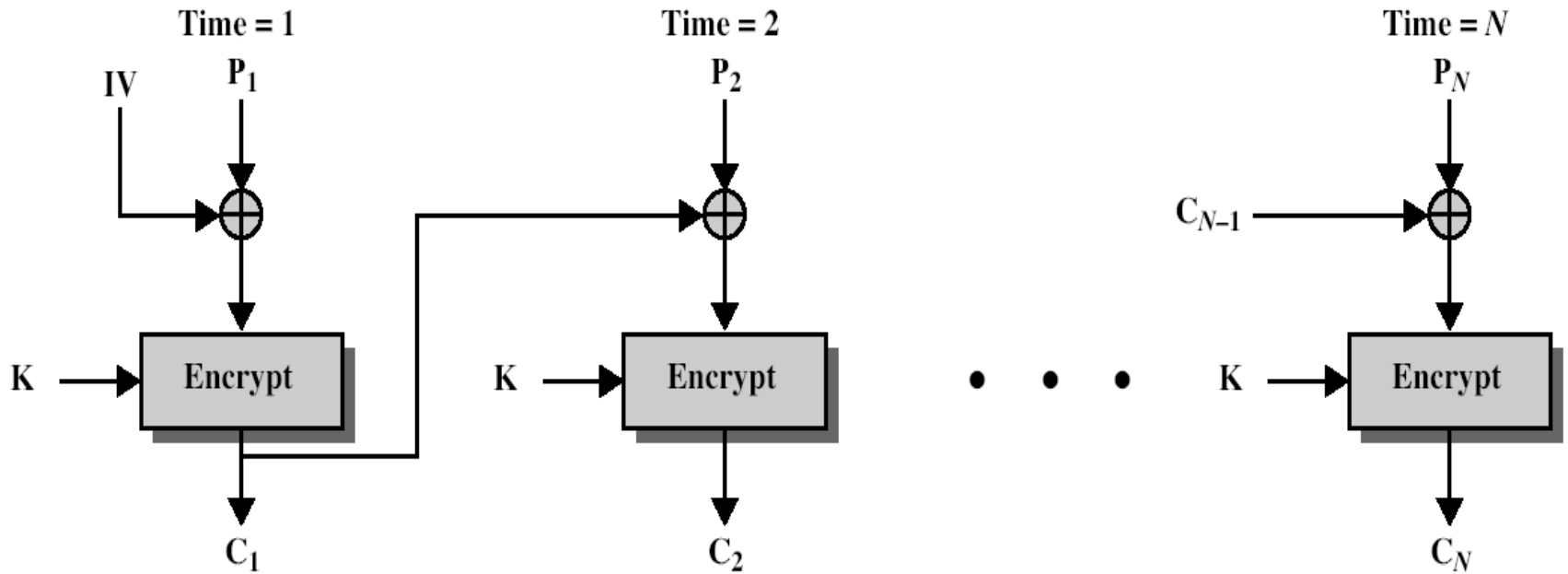
- At end of message must handle a possible last block, which is not as large as block size of cipher

Message Padding

- At end of message must handle a possible last block, which is not as large as block size of cipher
  - Pad either with known non-data value (eg nulls)
  - Or pad last block along with count of pad size
    - eg. [b1 b2 b3 0 0 0 0 5] - 3 data bytes, 5 bytes pad+count

Advantages and Limitations of CBC

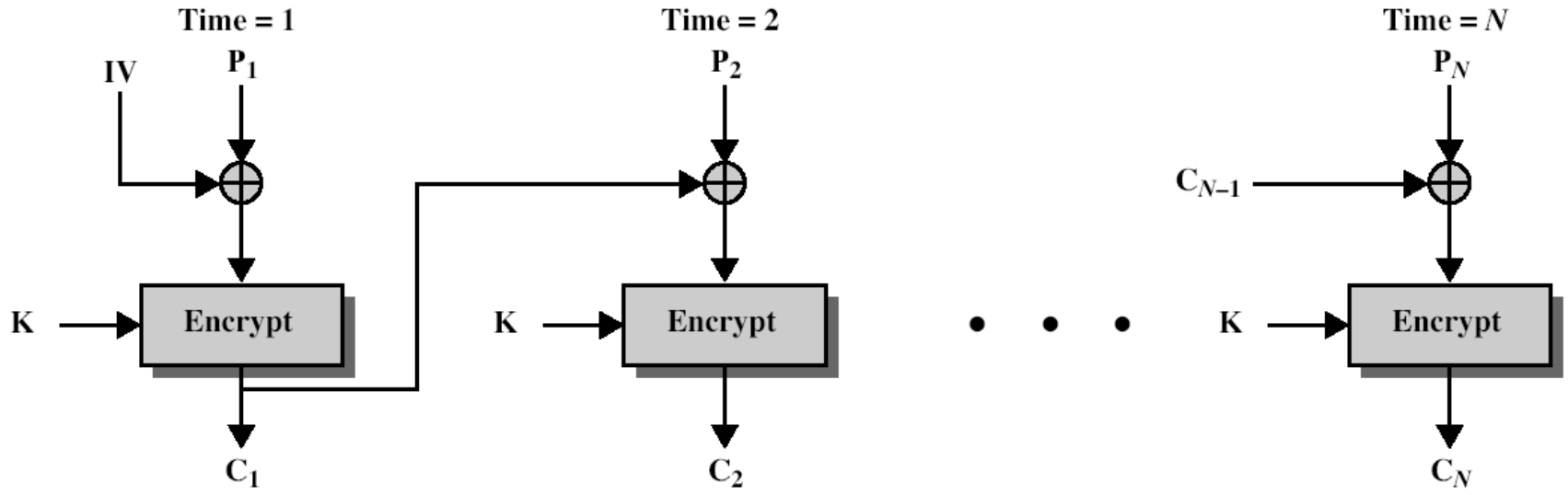
- Advantage:
  - Avalanche effect: A ciphertext block depends on all blocks before it - any change to one block affects all the following ciphertext blocks



(a) Encryption

Advantages and Limitations of CBC

- Disadvantage:
  - Encryption is sequential (i.e., cannot be parallelized)
  - Need Initialization Vector (IV)
    - Which must be known to sender & receiver
    - IV must either be a fixed value or be sent encrypted in ECB mode before rest of message



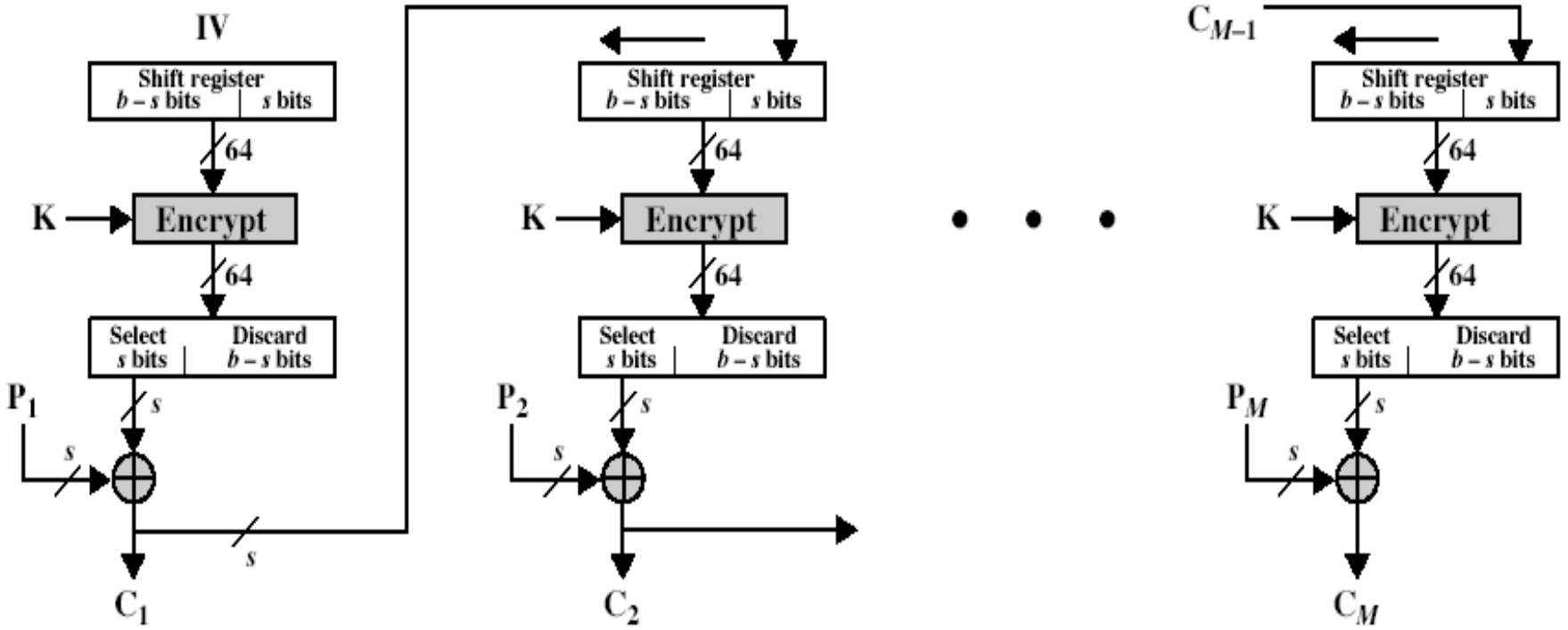
(a) Encryption

Cipher FeedBack Mode (CFB)

- When the data unit is smaller than the block size (e.g. data is only available a bit/byte at a time).
- Convert AES/DES into a stream cipher that can be used to encrypt any number of bits
  - Property of stream cipher: the ciphertext is of the same length as the plaintext.
  - Eliminates the need to pad a mesg.

Cipher FeedBack Mode (CFB): Encryption

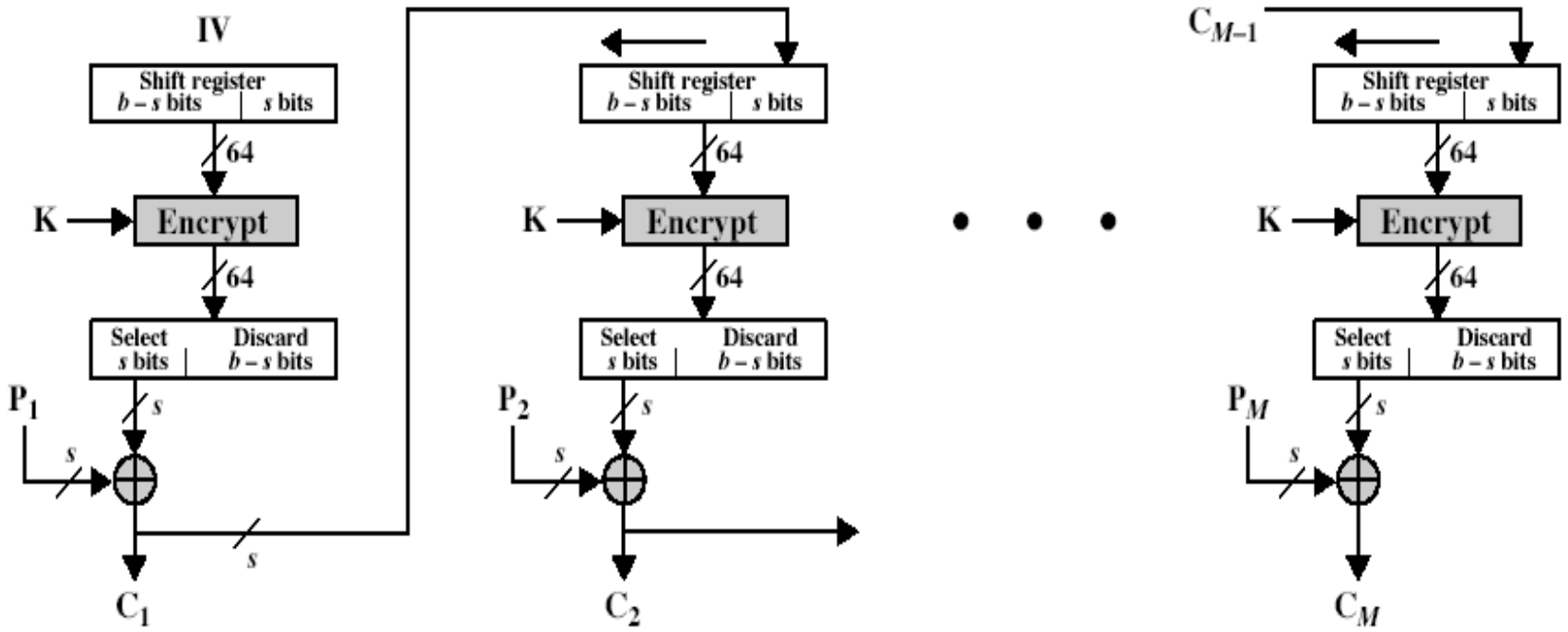
- E.g. The unit of transmission is s bits.
  - 64-bit shift register is initially set to some initialization vector (IV).
  - The leftmost s bits of the output of the encryption function is XORed with the first unit of plaintext **P1** to produce **C1**.



(a) Encryption

Cipher FeedBack Mode (CFB): Encryption

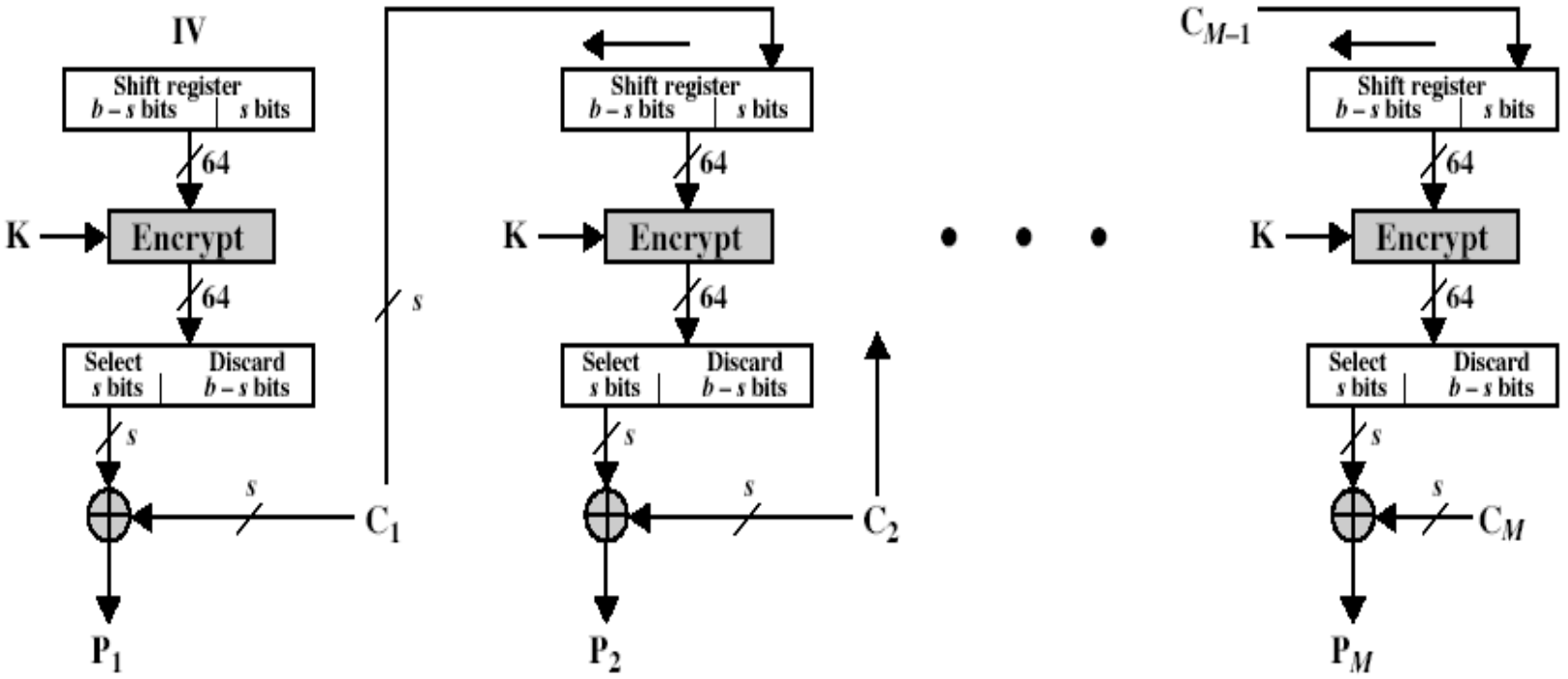
- E.g. the unit of transmission is s bits.
  - The contents of the shift register are shifted left by s bits and C1 is placed in the rightmost s bits of the shift register.
  - Continue this process until all plaintext units have been encrypted.



(a) Encryption

Cipher Feedback Mode (CFB): Decryption

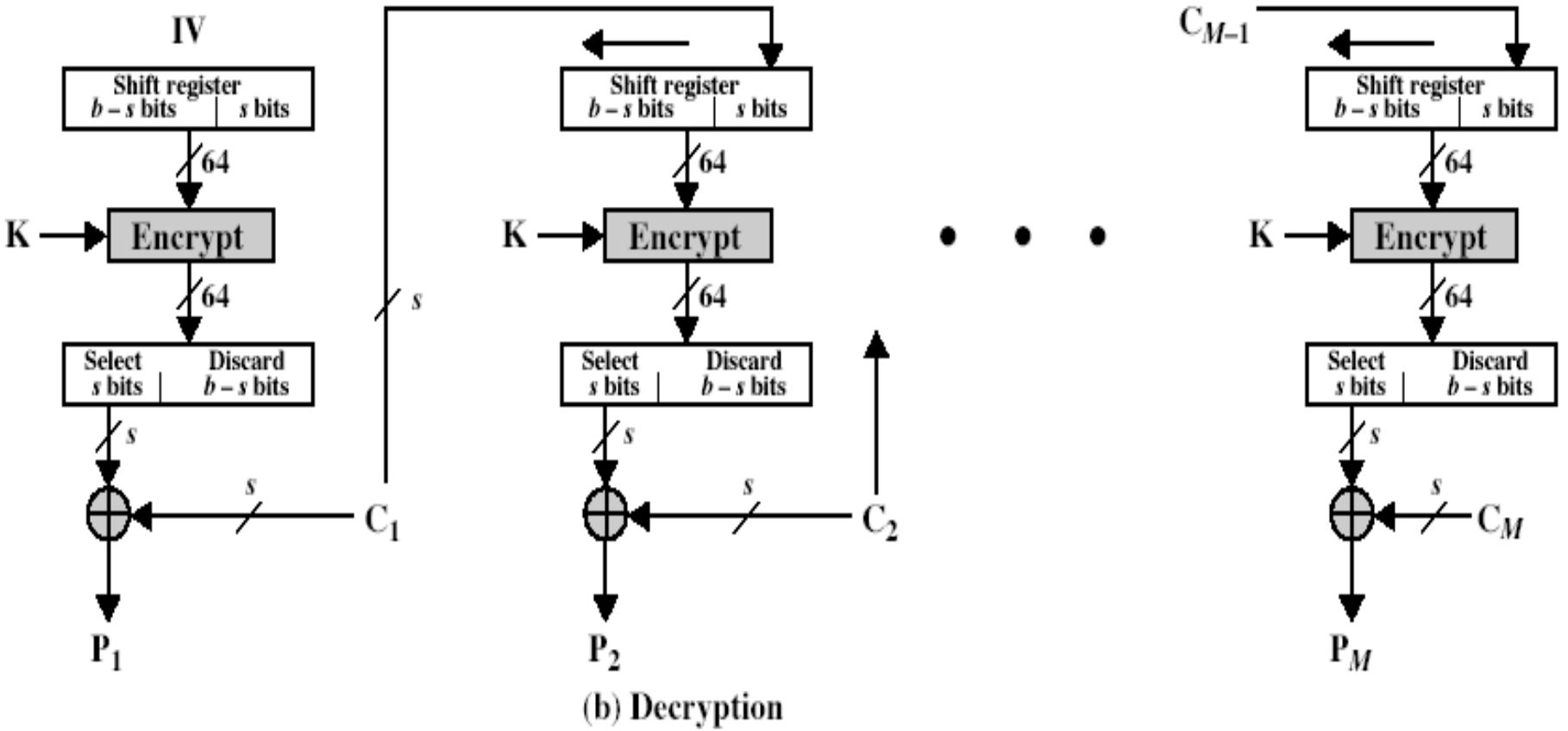
- E.g. the unit of transmission is s bits.
  - Same scheme as encryption, except that the received ciphertext unit is XORed with the output of the encryption function to produce the plaintext unit.



(b) Decryption

Cipher FeedBack Mode (CFB): Decryption

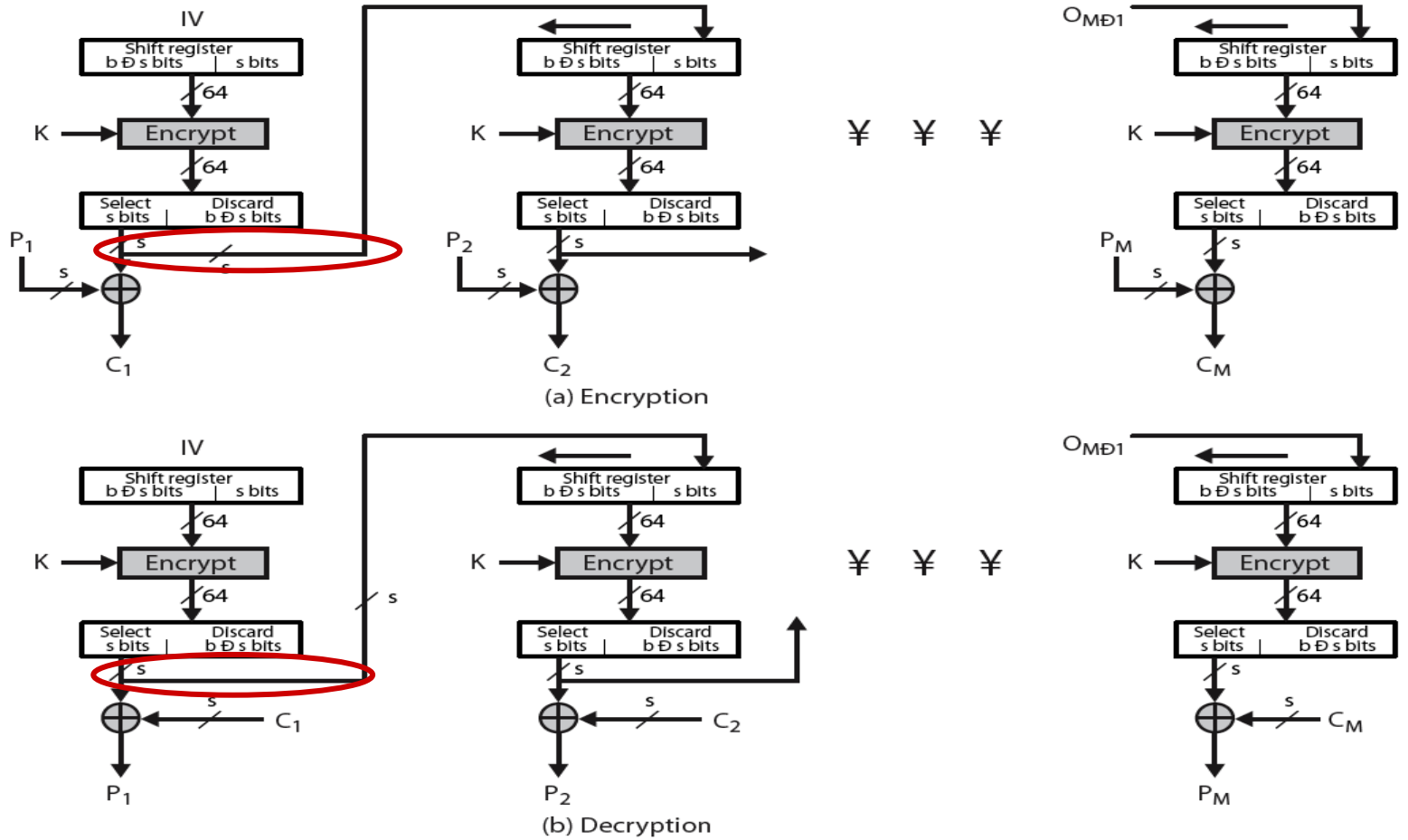
- Question: how to prove that the decryption is correct?



(b) Decryption

Output FeedBack (OFB)

- In OFB, the output of the encryption function is fed back to the shift register, while in CFB, the ciphertext unit is fed back to the register.

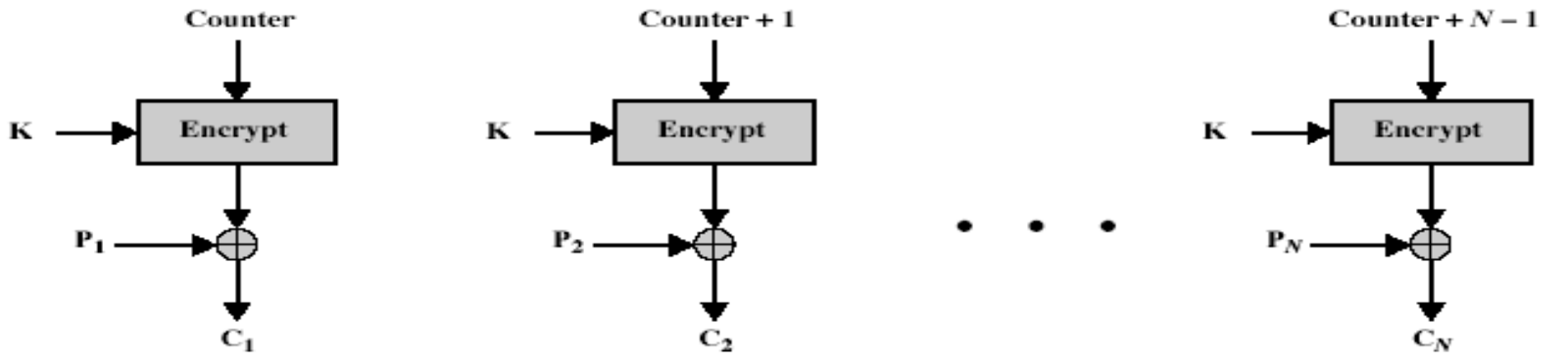


Advantage: OFB

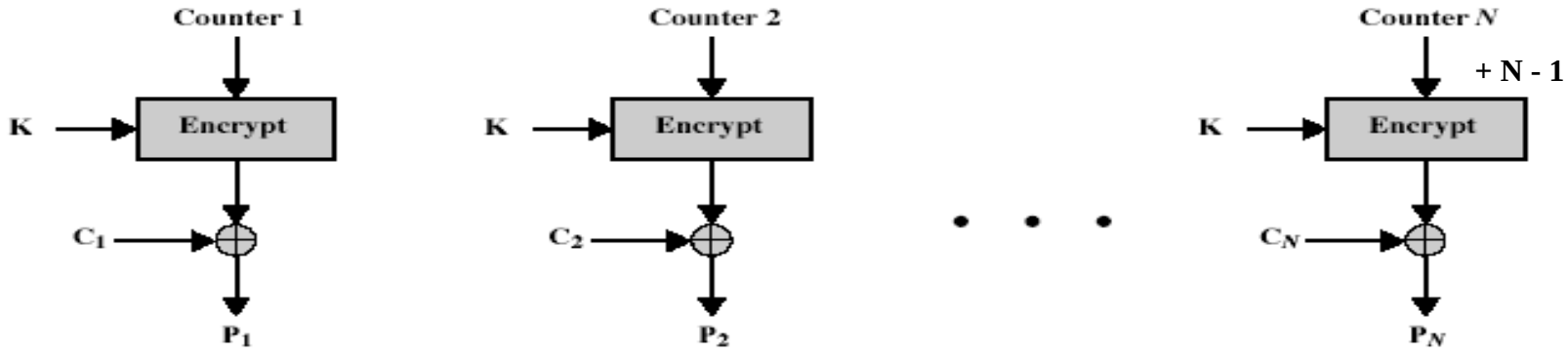
- Bit errors in transmission do not propagate
  - E.g. if a bit error occurs in C1, only the recovered value of P1 is affected.
  - When using CFB, C1 is the input to the shift register and may corrupt the subsequent plaintext units.

Counter (CTR)

- The counter is initialized to some value and then incremented by 1 for each subsequent block.
- The counter can be any simple function which produces a sequence which is guaranteed not to repeat for a long time



(a) Encryption



(b) Decryption

Counter (CTR)

- The correctness of the decryption process

  Encryption: $C_j = E(K, \text{Counter} + j - 1) \oplus P_j$

  Decryption: $P_j = E(K, \text{Counter} + j - 1) \oplus C_j$

  Proof:

  $$A \oplus A = 0$$

  $$0 \oplus A = A$$

  $$\begin{aligned} P_j &= E(K, \text{Counter} + j - 1) \oplus C_j \\ &= E(K, \text{Counter} + j - 1) \oplus E(K, \text{Counter} + j - 1) \oplus P_j \\ &= 0 \oplus P_j \\ &= P_j \end{aligned}$$

Advantages and Requirements of CTR

- Advantages:
  - Efficiency:
    - Encryption/decryption can be done in parallel on multiple blocks of plaintext or ciphertext
    - The execution of the encryption algorithm does not depend on the plaintext and ciphertext - can preprocess in advance.
    - Good for high-speed network encryptions
  - Random access to encrypted data blocks
  - Provable security (good as other modes)
- Security Requirement: The same counter value should not be used multiple times.

Summary: Comparison of Block Cipher Modes

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
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

Credits

- Many slides borrowed from Dr. Ping Yang from State University of New York at Binghamton.