Encryption Modes

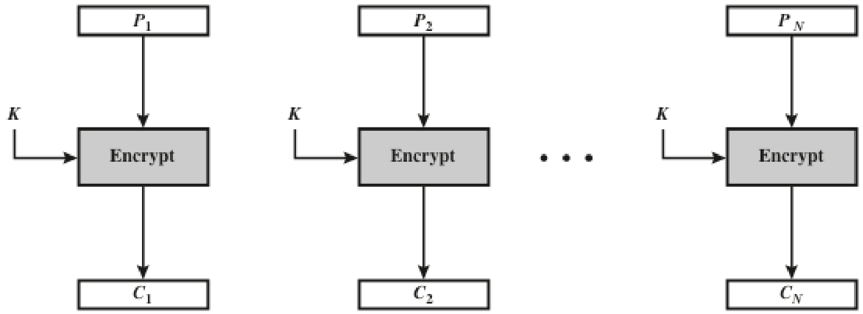
Outline

- Electronic Code Book mode (ECB)
- Cipher Block Chaining mode (CBC)
- Output Feedback mode (OFB)
- Cipher Feedback mode (CFB)
- Counter mode (CTR)

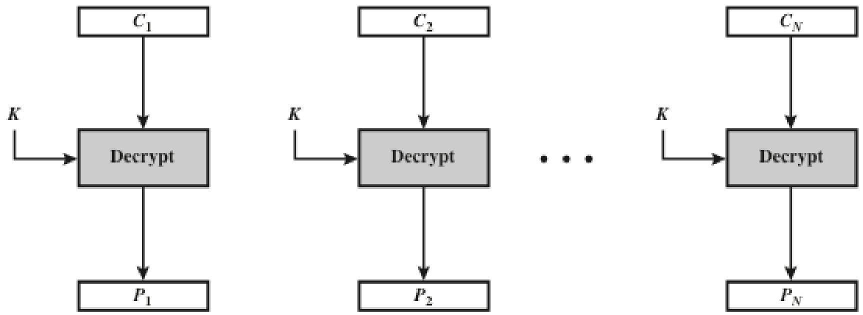
Electronic Code Book mode (ECB)

- How to encode multiple blocks of a long message?
- Each block is encrypted independently of the others

$$C_i = E_K(P_i)$$



(a) Encryption



(b) Decryption

ECB: advantages/disadvantages

- **Advantages**
  - no block synchronization between sender and receiver is required
  - bit errors caused by noisy channels only affect the corresponding block but not succeeding blocks
  - Encryption/decryption can be parallelized => high-speed
- **Disadvantages**
  - ECB encrypts highly deterministically
    - identical plaintexts result in identical ciphertexts
    - an attacker recognizes if the same message has been sent twice

Substitution Attack on ECB

- Once a particular plaintext to ciphertext block mapping $P_i \rightarrow C_i$ is known, a sequence of ciphertext blocks can easily be manipulated
- Suppose an *electronic bank transfer*

Block #	1	2	3	4	5
	Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount $

  - the encryption key between the two banks does not change too frequently
  - The attacker sends $1 transfers from his account at bank A to his account at bank B repeatedly
    - He can check for ciphertext blocks that repeat, and he stores blocks 1,3 and 4 of these transfers
  - He now simply replaces block 4 of other transfers with the block 4 that he stored before
    - *all transfers* from some account of bank A to some account of bank B are redirected to go into the attacker’s B account!

Cipher Block Chaining mode (CBC)

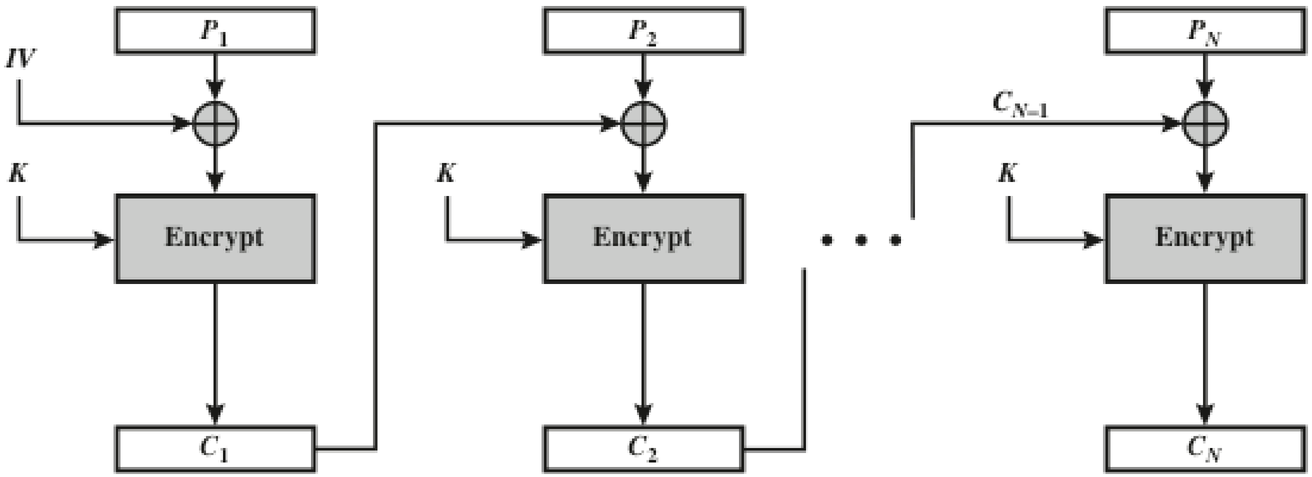
- There are two main ideas behind the CBC mode:
  - Previous cipher block is chained with current plaintext block
    - ciphertext C_i depends not only on block P_i but on ciphertext block C_{i-1} as well
  - The encryption is randomized by using an Initialization Vector (IV)

$$C_1 = E_K(P_1 \oplus IV)$$

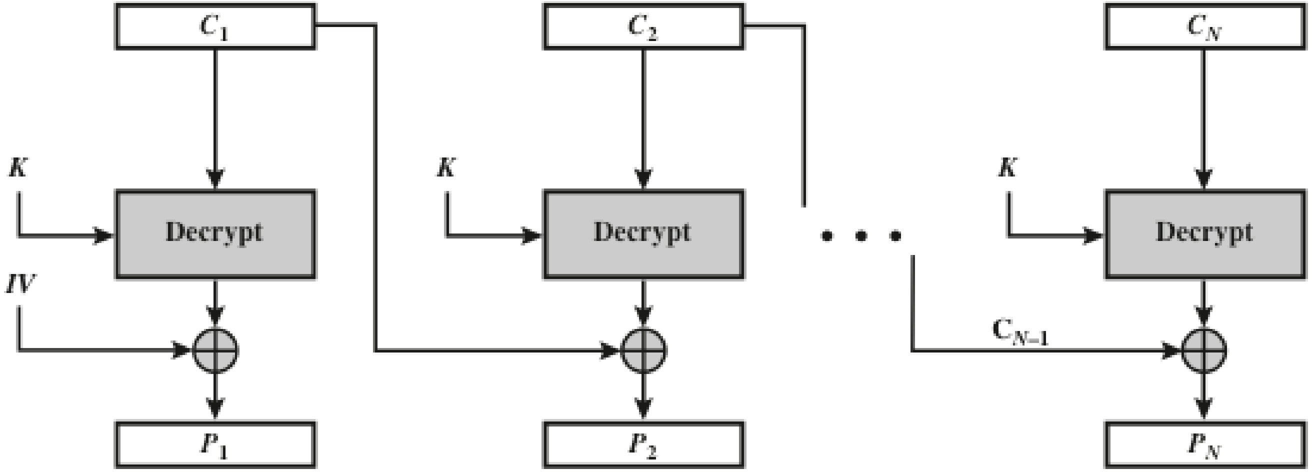
$$C_i = E_K(P_i \oplus C_{i-1})$$

- IV should be a **non-secret nonce** (used only once) value => the CBC mode becomes a probabilistic encryption scheme, i.e., two encryptions of the same plaintext look entirely different

Cipher Block Chaining mode (CBC)



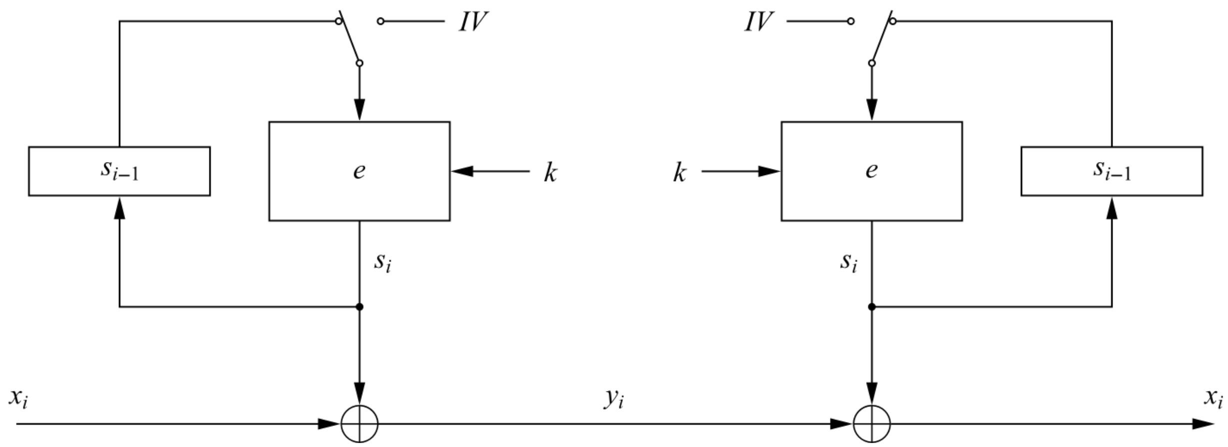
(a) Encryption



(b) Decryption

Output Feedback mode (OFB)

- It is used to build a *synchronous* **stream cipher** from a block cipher
- The key stream is not generated bitwise but instead in a blockwise fashion
- The output of the cipher gives us key stream bits S_i with which we can encrypt plaintext bits using the XOR operation



Encryption (first block): $s_1 = e_k(\mathrm{IV})$ *and* $y_1 = s_1 \oplus x_1$

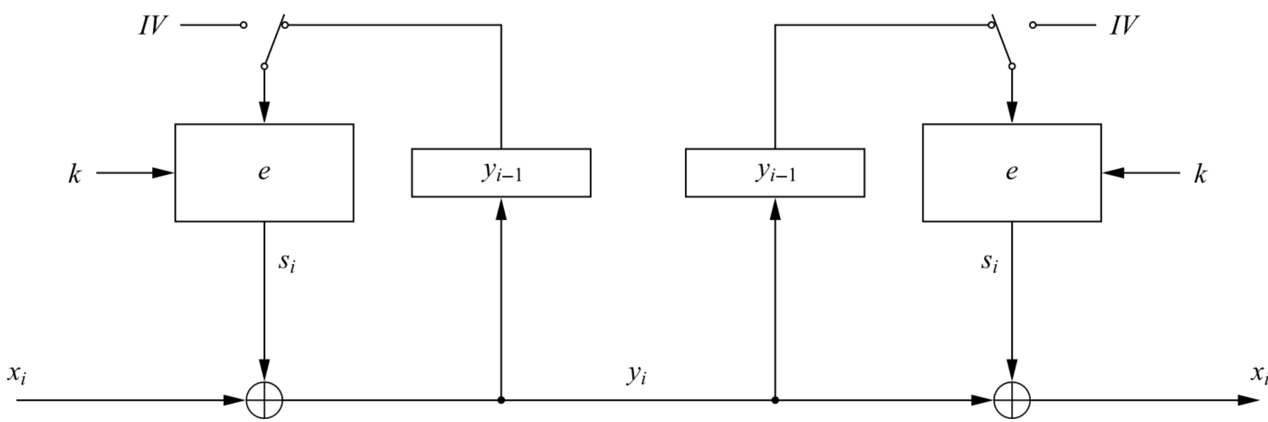
Encryption (general block): $s_i = e_k(s_{i-1})$ *and* $y_i = s_i \oplus x_i\,,\quad i \geq 2$

Decryption (first block): $s_1 = e_k(\mathrm{IV})$ *and* $x_1 = s_1 \oplus y_1$

Decryption (general block) : $s_i = e_k(s_{i-1})$ *and* $x_i = s_i \oplus y_i\,,\quad i \geq 2$

Cipher Feedback mode (CFB)

- It uses a block cipher as a building block for an asynchronous **stream cipher** (similar to the OFB mode), more accurate name: “Ciphertext Feedback Mode”
- The key stream S_i is generated in a blockwise fashion and is also a function of the ciphertext
- As a result of the use of an IV, the CFB encryption is also nondeterministic

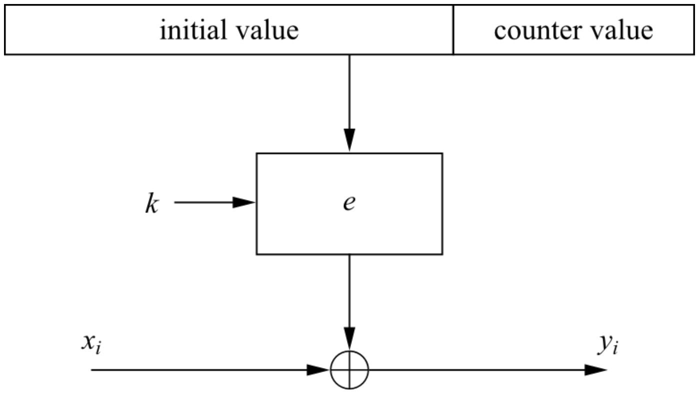


Encryption (first block): $y_1 = e_k(\mathrm{IV}) \oplus x_1$
Encryption (general block): $y_i = e_k(y_{i-1}) \oplus x_i, \quad i \geq 2$
Decryption (first block): $x_1 = e_k(\mathrm{IV}) \oplus y_1$
Decryption (general block) : $x_i = e_k(y_{i-1}) \oplus y_i, \quad i \geq 2$

- It can be used in situations where short plaintext blocks are to be encrypted

Counter mode (CTR)

- It uses a block cipher as a **stream cipher** (like the OFB and CFB modes)
- The key stream is computed in a blockwise fashion
- The input to the block cipher is a counter which assumes a different value every time the block cipher computes a new key stream block



Encryption: $y_i = e_k(\text{IV} \,||\, \text{CTR}_i) \oplus x_i, \quad i \geq 1$

Decryption : $x_i = e_k(\text{IV} \,||\, \text{CTR}_i) \oplus y_i, \quad i \geq 1$

- Unlike CFB and OFB modes, the CTR mode can be parallelized since the 2nd encryption can begin before the 1st one has finished
  - Desirable for high-speed implementations, e.g., in network routers

Summary

- There are many different ways to encrypt with a block cipher. Each mode of operation has some advantages and disadvantages
- Several modes turn a block cipher into a stream cipher
- The straightforward ECB mode has security weaknesses, independent of the underlying block cipher
- The counter mode allows parallelization of encryption and is thus suited for high speed implementations

- Wikipedia
  - http://en.wikipedia.org/wiki/Modes_of_operation