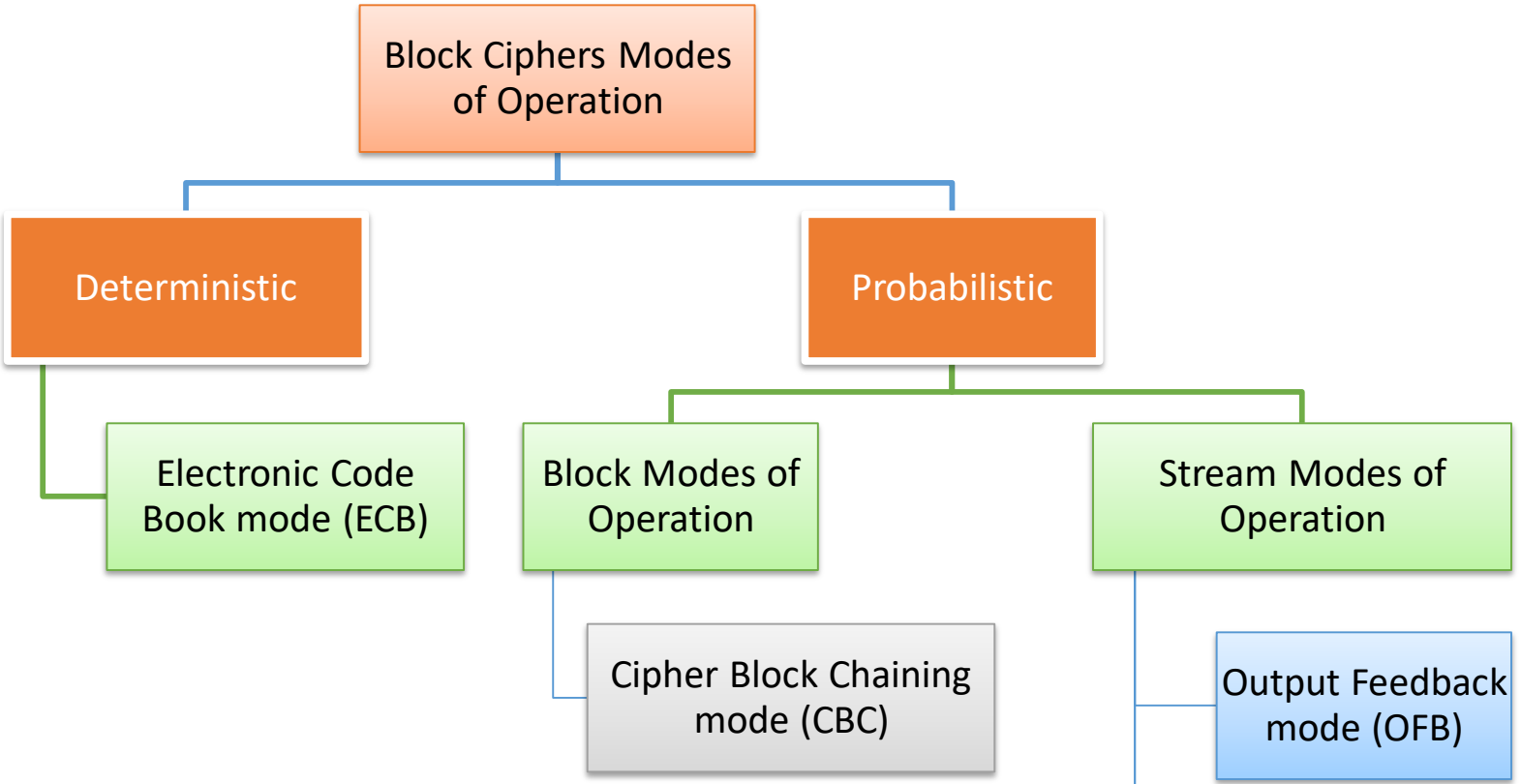
Block Ciphers Modes of Operation

Outline

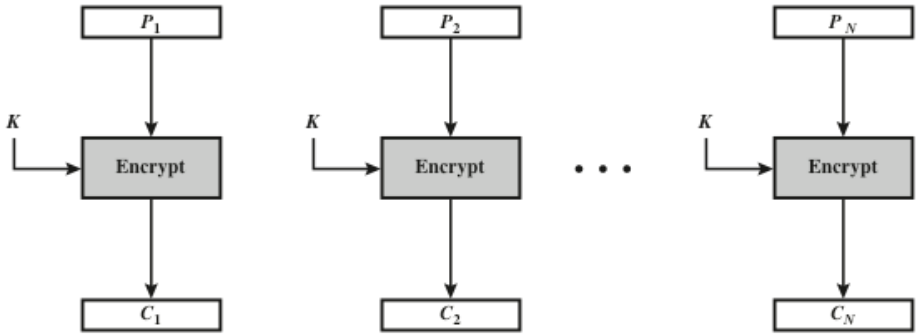


- Deterministic – PT is mapped to fixed CT if the key is unchanged
- Probabilistic – Uses randomness to achieve non-deterministic generation of the CT

ECB & CBC

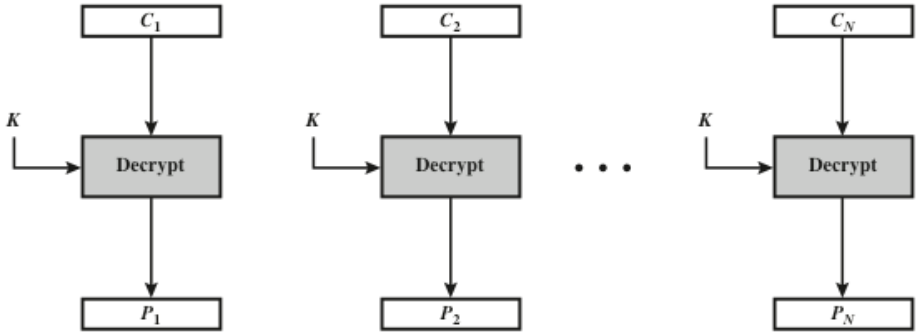
Electronic Code Book mode (ECB)

- How to encrypt multiple blocks of a long message?
  - We need to break up the data into blocks and then encrypt them
  - The way we do this impacts security
- ECB = Each block is encrypted **independently** of the others



(a) Encryption

$$C_i = E_K(P_i)$$



(b) Decryption

$$P_i = E_K^{-1}(C_i)$$

ECB advantages/disadvantages

- **Advantages**
  - Bit errors caused by noisy channels only affect the corresponding block but not succeeding blocks
  - Encryption/decryption can be parallelized => high-speed
- **Disadvantages**
  - ECB is a deterministic encryption scheme
    - Identical PT blocks produce the same CT blocks
    - 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 sored 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)

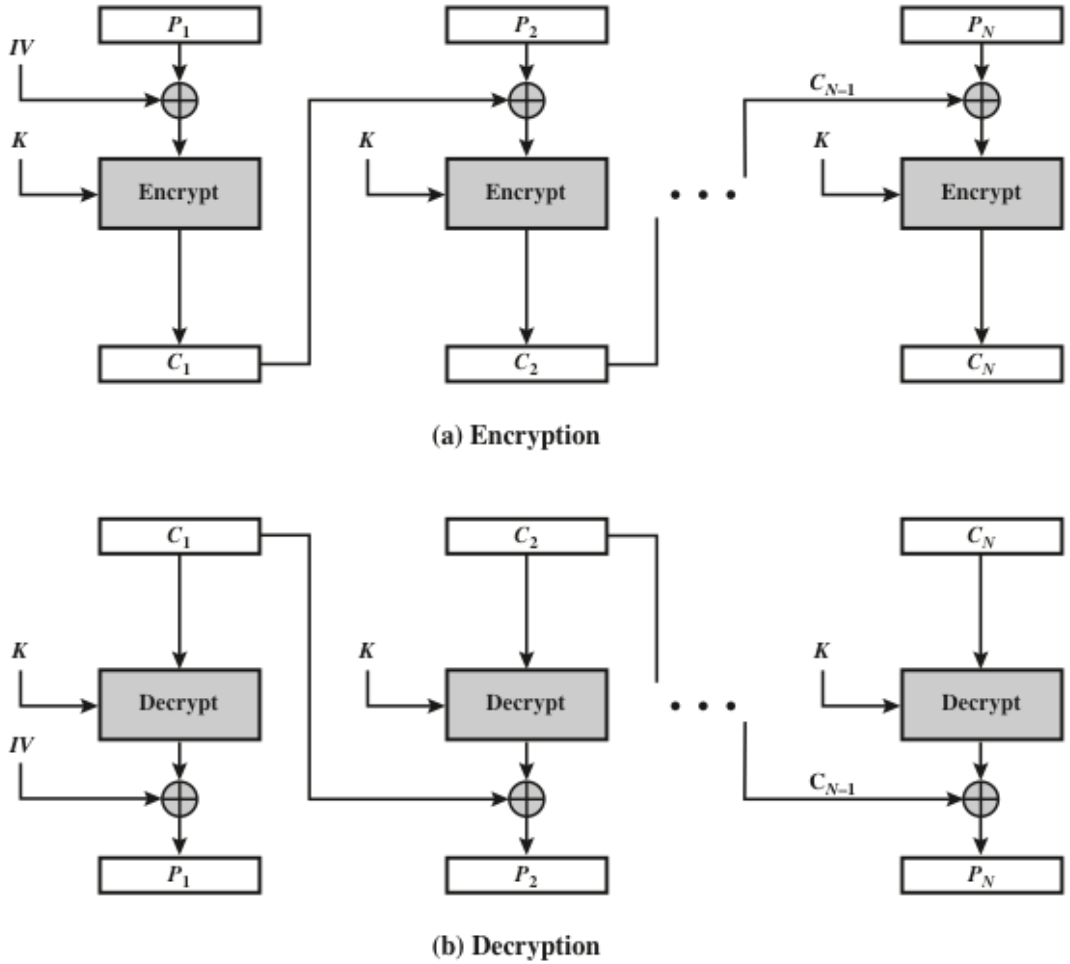
- There are two main ideas behind the CBC mode:
  - Previous cipher block is chained with current plaintext block
    - Ciphertext C_i depends not only on block P_i but also on ciphertext block C_{i-1}
    - Any change to a block affects all following ciphertext blocks
  - The encryption is randomized 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** (number used only once) => the CBC mode becomes a **probabilistic** encryption scheme, i.e., two encryptions of the same plaintext look entirely different

Cipher Block Chaining mode (CBC)



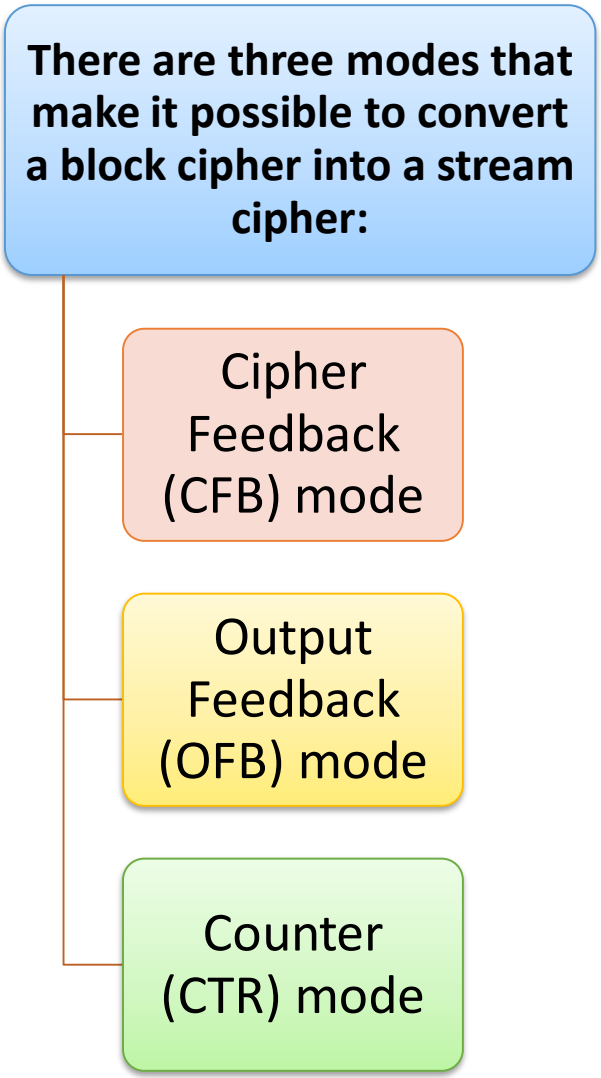
But

- Sequential implementation. Cannot be parallelized.
- If one PT block changes => must re-encrypt all following blocks

Stream Modes of Operation

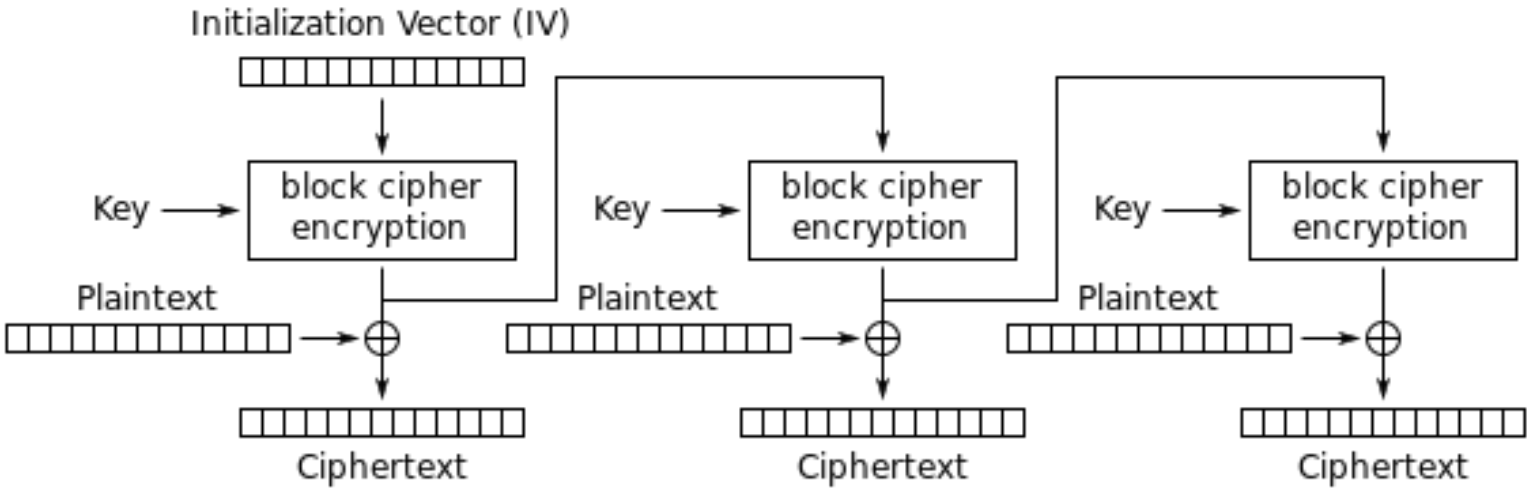
Stream Modes of Operation

- Use block cipher as some form of pseudo-random number generator
  - The random number bits are then XOR'ed with the plaintext (as in stream cipher)
  - The key stream is computed in a **blockwise** fashion (instead of bitwise)
  - The key stream block has the same size as the plaintext block



Output Feedback mode (OFB)

- It is used to build a **stream cipher** from a block cipher
- The output of the cipher gives us key stream bits S_i with which we can use to encrypt plaintext bits using the XOR operation.
  - Output of the cipher is feed back for next stage



Encryption (first block): $S_1 = e_k(IV)$ and $C_1 = S_1 \oplus P_1$

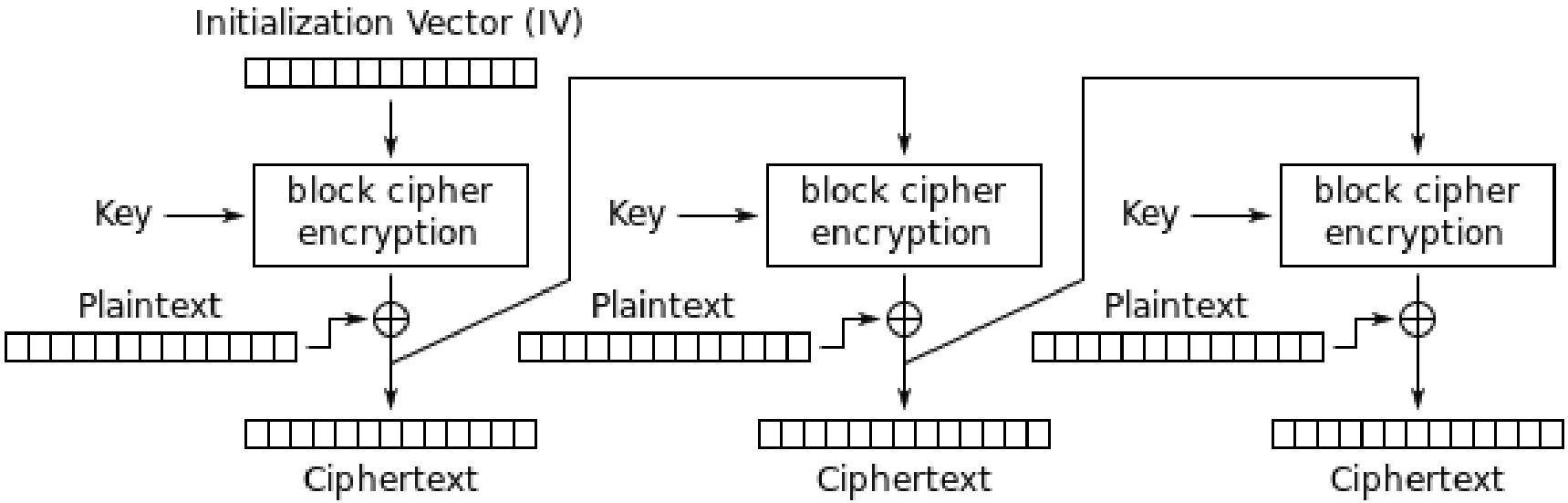
Encryption (general block): $S_i = e_k(S_{i-1})$ and $C_i = S_i \oplus P_i$, $i \geq 2$

Decryption (first block): $S_1 = e_k(IV)$ and $P_1 = S_1 \oplus C_1$

Decryption (general block) : $S_i = e_k(S_{i-1})$ and $P_i = S_i \oplus C_i$, $i \geq 2$

Cipher Feedback mode (CFB)

- The key stream S_i is generated based the ciphertext C_{i-1}
- As a result of IV, the CFB encryption is also nondeterministic



Encryption (first block): $C_1 = e_k(IV) \oplus P_1$

Encryption (general block): $C_i = e_k(C_{i-1}) \oplus P_i, \quad i \geq 2$

Decryption (first block): $P_1 = e_k(IV) \oplus C_1$

Decryption (general block) : $P_i = e_k(C_{i-1}) \oplus C_i, \quad i \geq 2$

Counter mode (CTR)

- It uses a block cipher as a **stream cipher** (like the OFB and CFB modes)
- Encrypt counter value rather than any feedback value
- The input to the block cipher is a counter value (same size as the plaintext block size) which must be different for each plaintext block that is encrypted

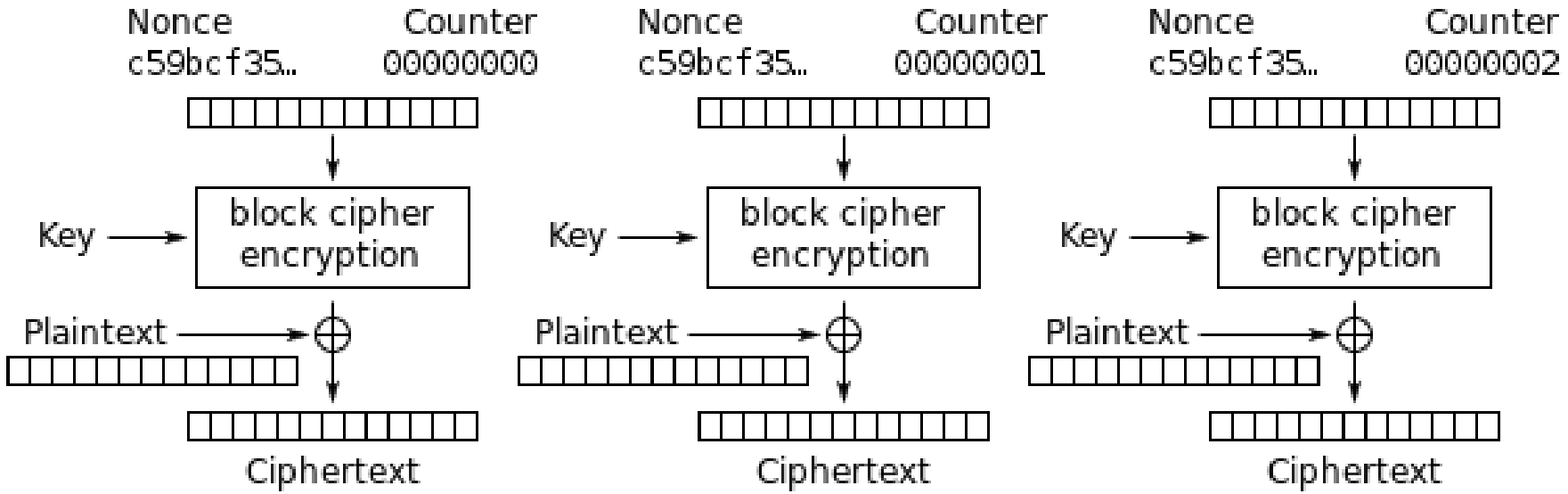
$$S_i = E_K(CTR_i)$$

$$C_i = P_i \oplus S_i$$

- The *keystream* is generated by encrypting a sequence of *counter blocks*
- 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

Counter mode (CTR)

- A counter block consists of the concatenation of two pieces: **a fixed nonce** (set at initialization) + **a variable counter**, which gets increased by 1 for any subsequent counter block.



Summary

Mode	Description
Electronic Codebook (ECB)	Each PT block is encrypted independently using the same key.
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the PT block XOR the CT of previous block $\mathbf{C_i = E_K(P_i \oplus C_{i-1})}$ With $\mathbf{C_1 = E_K(P_1 \oplus IV)}$
Output Feedback (OFB)	Encryption of the preceding key stream to produce a pseudorandom output, which is XORed with PT block to produce CT block. With $\mathbf{S_1 = e_k(IV)}$
Cipher Feedback (CFB)	Encryption the preceding CT block to produce pseudorandom output, which is XORed with PT block to produce CT block. With $\mathbf{C_1 = e_k(IV) \oplus P_1}$
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block. $S_i = E_K(CTR_i)$ $C_i = P_i \oplus S_i$

Summary

- When using block ciphers to encrypt data larger than one block, you need to pick an operating mode
  - Each mode of operation has some advantages and disadvantages
  - Your choice impacts security and performance
- The straightforward ECB mode is vulnerable to substitution attack
- Several modes turn a block cipher into a stream cipher
- The counter mode allows parallelization of encryption and is thus suited for high speed implementations

References

- Block cipher modes of operation Wikipedia page
  - http://en.wikipedia.org/wiki/Modes_of_operation