Block Ciphers: Modes of Operation

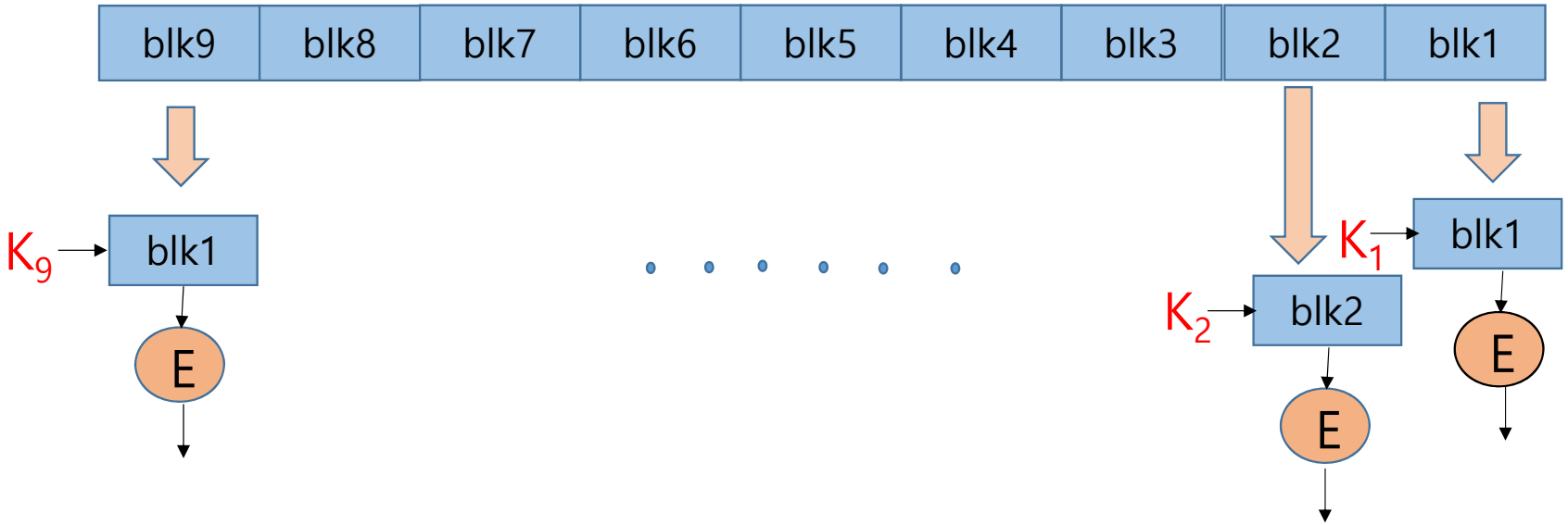
2019. 3. 19

Contents

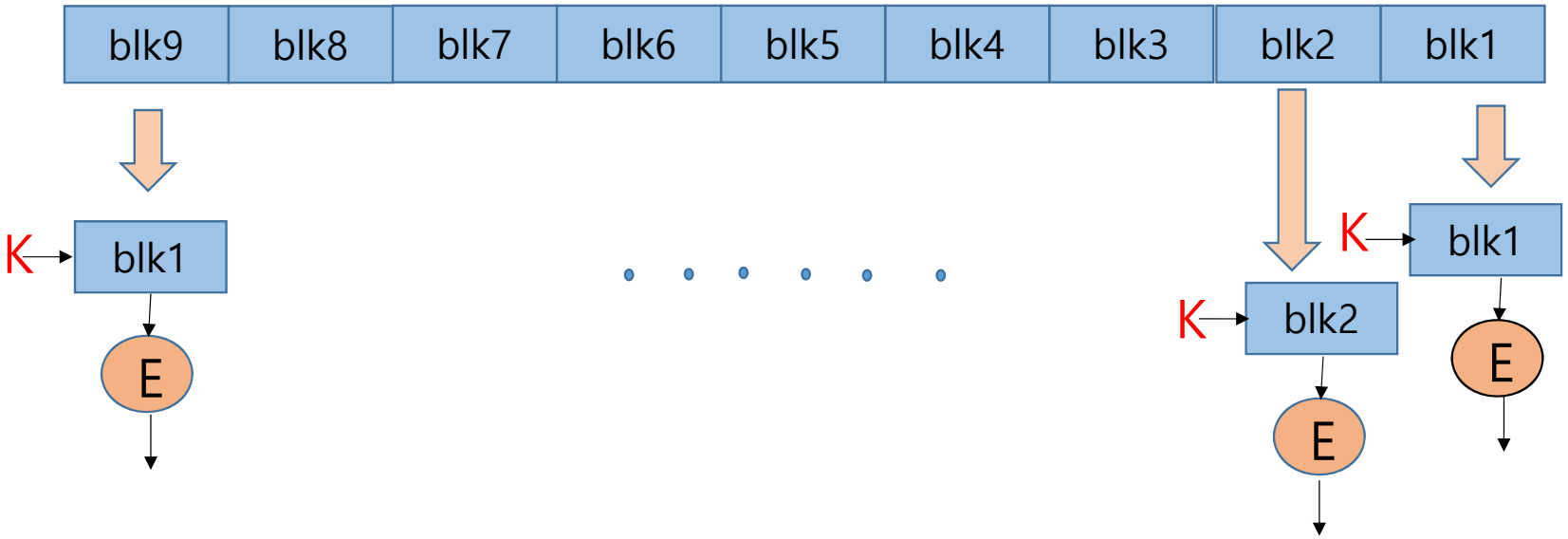
- Introduction to crypto
- Symmetric-key cryptography
  - Stream ciphers
  - Block ciphers
  - Block cypher operation modes
- Public-key cryptography
  - RSA
  - ECC
  - Digital signature
  - Public key Infrastructure
- Cryptographic hash function
  - Attack complexity
  - Hash Function algorithm
- Integrity and Authentication
  - Message authentication code
  - GCM
  - Digital signature
- Key establishment
  - server-based
  - Public-key based
  - Key agreement (Diffie-Hellman)

Encryption of multiple blocks

- What if a file have multiple block?
  - If we use different keys for each block, encryption is like one time pad(OTP).



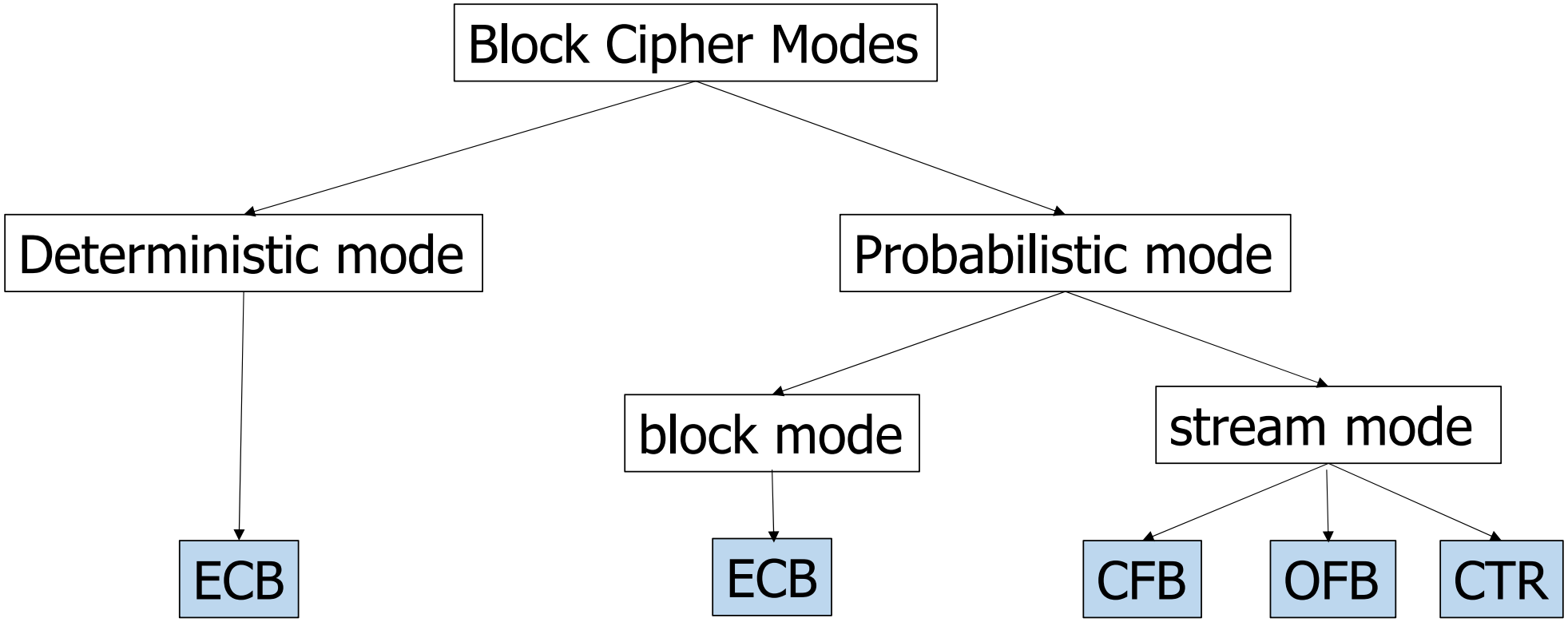
- What if we use the same key for all the blocks of the file? Are there any problems?



Modes of operation

- Block cipher modes of operation
  - ECB: Electronic code book
  - CBC: Cipher block chaining
  - CFB: Cipher feedback
  - OFB: Output feedback
  - CTR: Counter mode
  - and more

Classification of operation modes



ECB

- Mapping between blocks of plaintext and ciphertext is fixed as long as the key is same. (deterministic)
- It is like a traditional code book.

Key = Ki	
P_0	C_0
P_1	C_1
P_2	C_2
P_3	C_3
P_4	C_4
…	…

Advantages of ECB

- Block synchronization is unnecessary.
  - Receiver can decrypt the received blocks regardless of receiving other blocks.
- Bit errors affect only corresponding block, not succeeding blocks.
- Encryption/decryption processes can be parallelized.

ECB weakness

- Suppose $P_i = P_j$
- Then $C_i = C_j$ and an attacker knows $P_i = P_j$
- This gives the attacker some information, even if he does not know P_i or P_j
- He might know P_i
- Is this a serious issue?

Substitution attack

- Consider the following plaintext.

  `"Abel loves Bob. Cain hates Tom."`

- Suppose the block size is 64-bits:

Abel lov	es Bob.	Cain hat	es Tom.
P_0	P_1	P_2	P_3

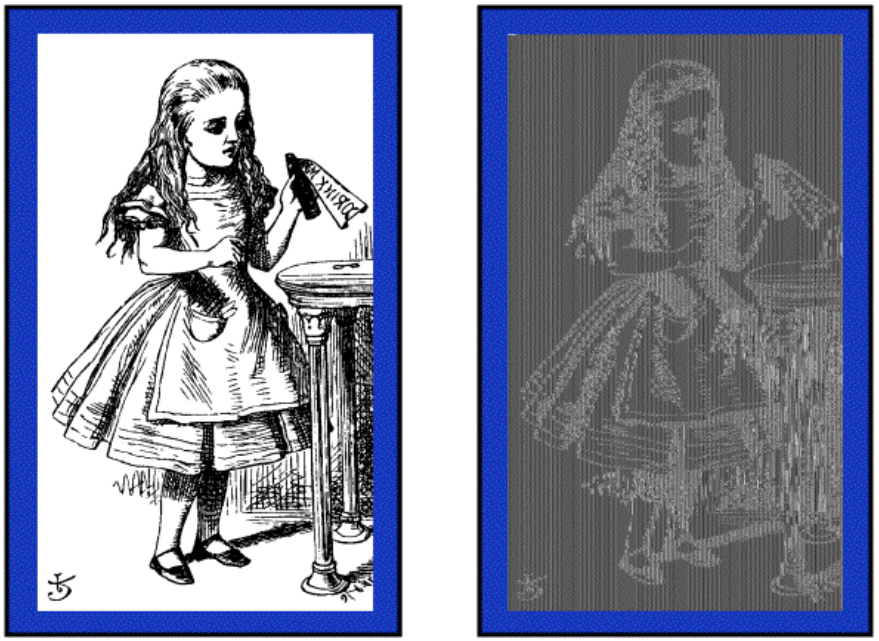
- Then, the cipher texts are C_0, C_1, C_2, C_3.
- Attacker reordered the cipher text blocks: C_0,C_3,C_2,C_1
- Then the decrypted plaintext is:

  `"Abel loves Tom. Cain Hates Bob. "`

- Still, attacker does not know contents about the ciphertext.

An Example of ECB encryption

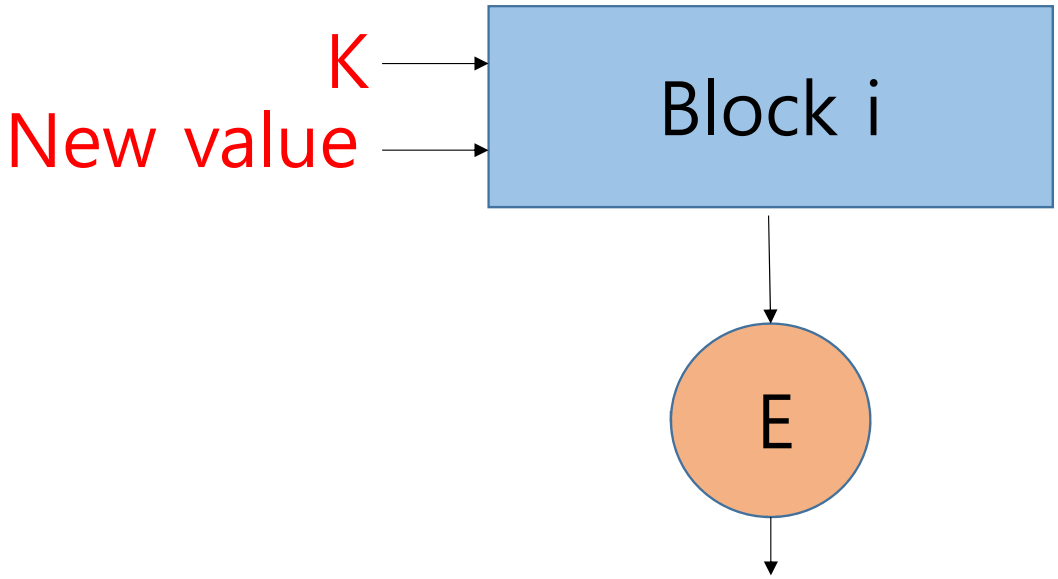
- Alice's uncompressed image, and ECB encrypted (TEA)



- Why does this happen?

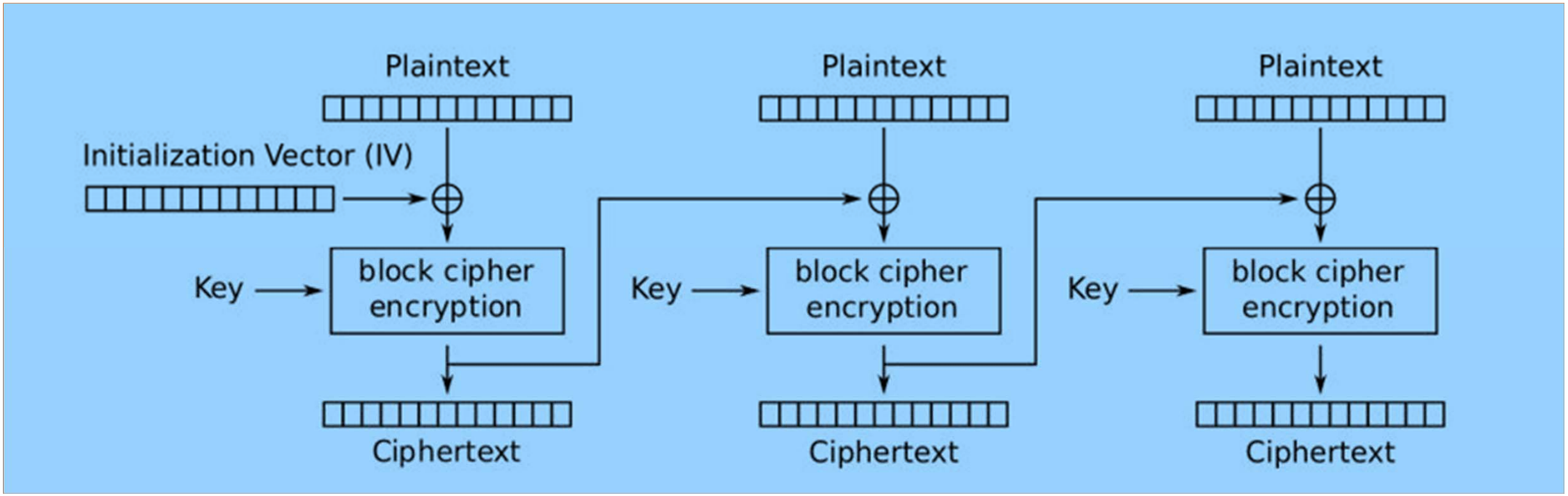
(source: Information Security of M. Stamp)

Fix the problem



CBC(Cipher block chaining) Encryption

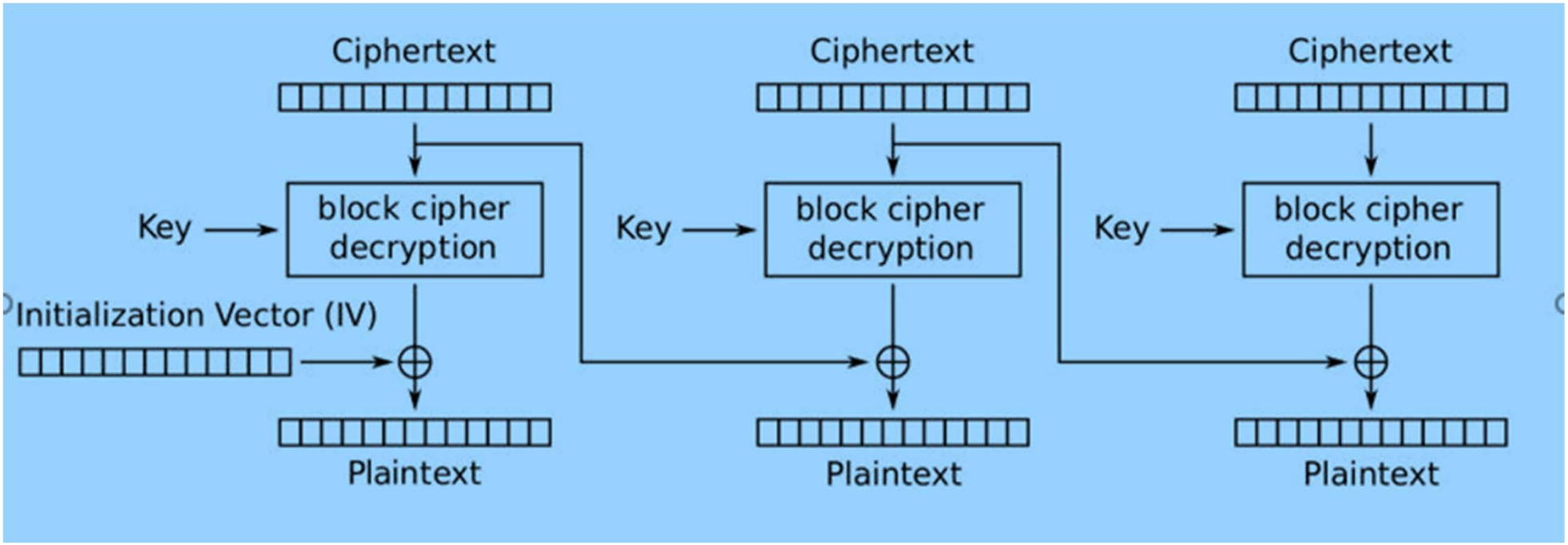
$C_0 = E_K(IV \oplus P_0)$, $C_1 = E_K(C_0 \oplus P_1)$, $C_2 = E_K(C_1 \oplus P_2)$,…



(source: Wikipedia)

CBC Decryption

$P_0 = D_K(C_0) \oplus IV,\ P_1 = D_K(C_1) \oplus C_0,\ P_2 = D_K(C_2) \oplus C_1, \ldots$



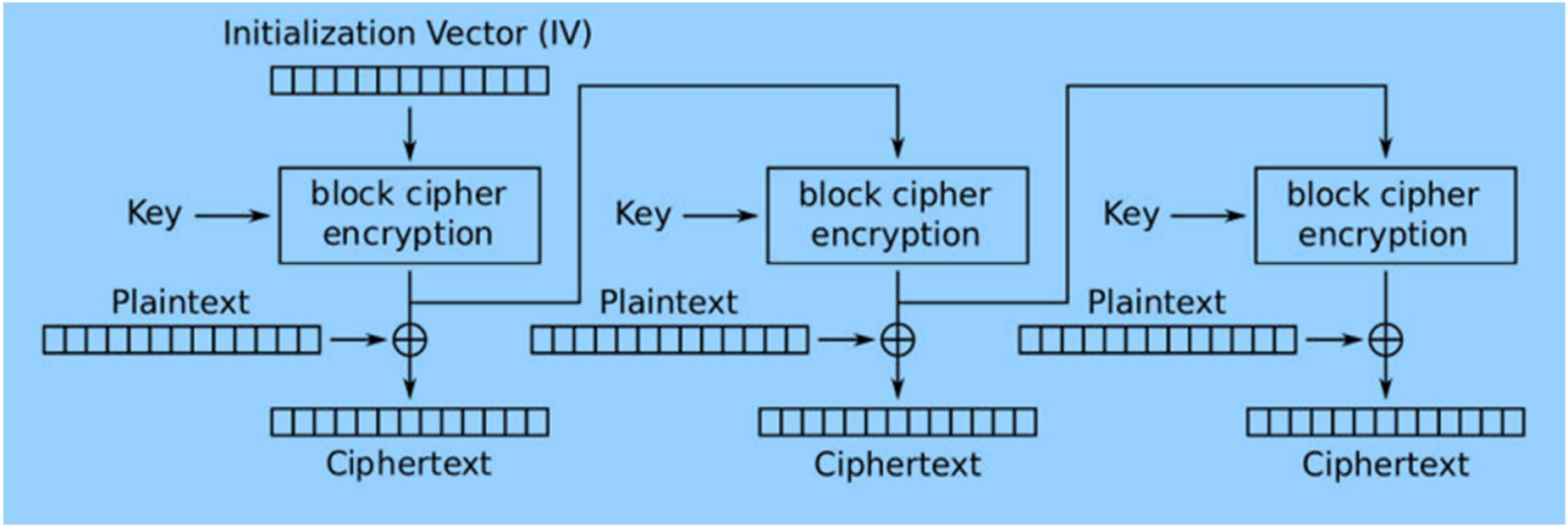
(source: Wikipedia)

CBC

- CBC encryption is probabilistic.
  - If we use new IV every time we encrypt, two ciphertexts of the same plaintext blocks are completely different.
- IV should be nonce. (should be used only once)
- But it should not be secret.(doesn’t need to be)

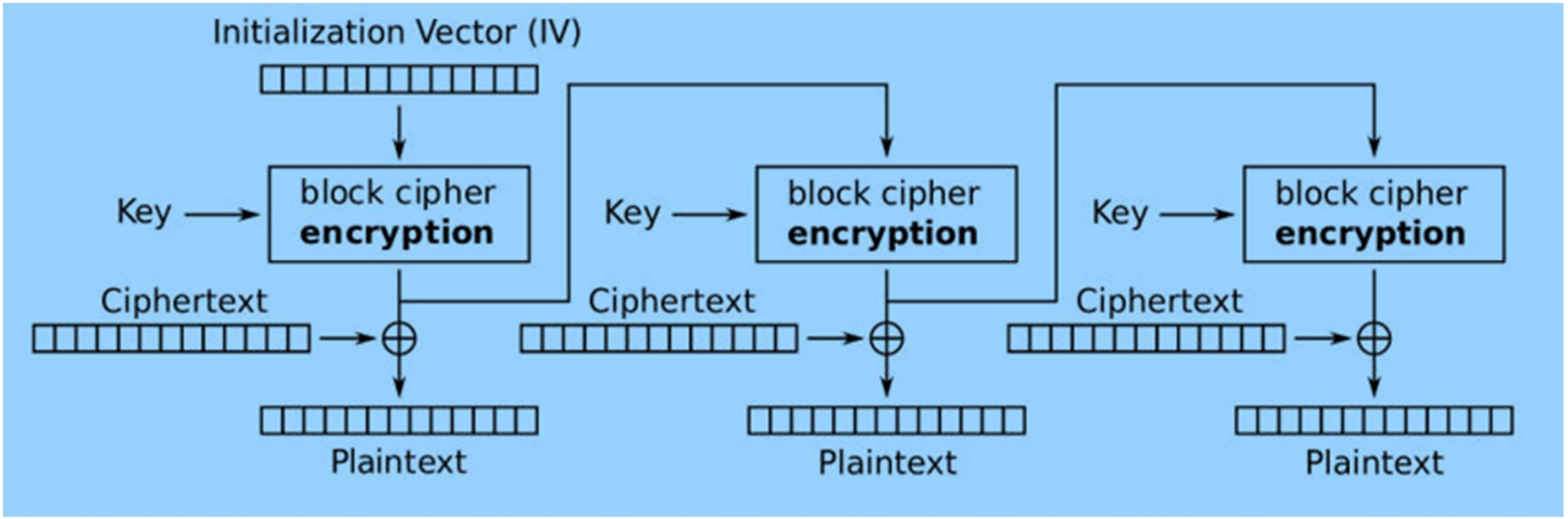
OFB Encryption

$I_0 = IV$, $O_i = E_K(I_i)$, $I_i = O_{i-1}$, $C_i = P_i \oplus O_i$, $P_i = C_i \oplus O_i$,…
It works like the stream cipher.
The key stream is generated block by block, not bitwise.



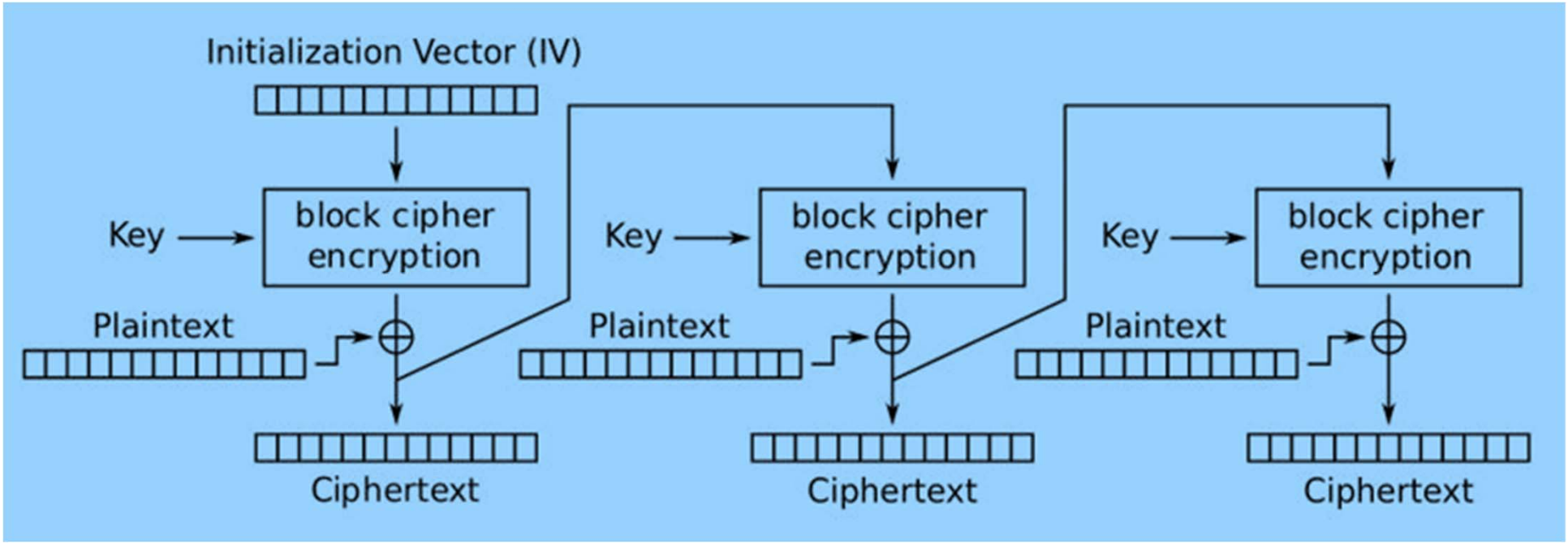
OFB Decryption

Note that when decrypting, block cipher uses the encryption.

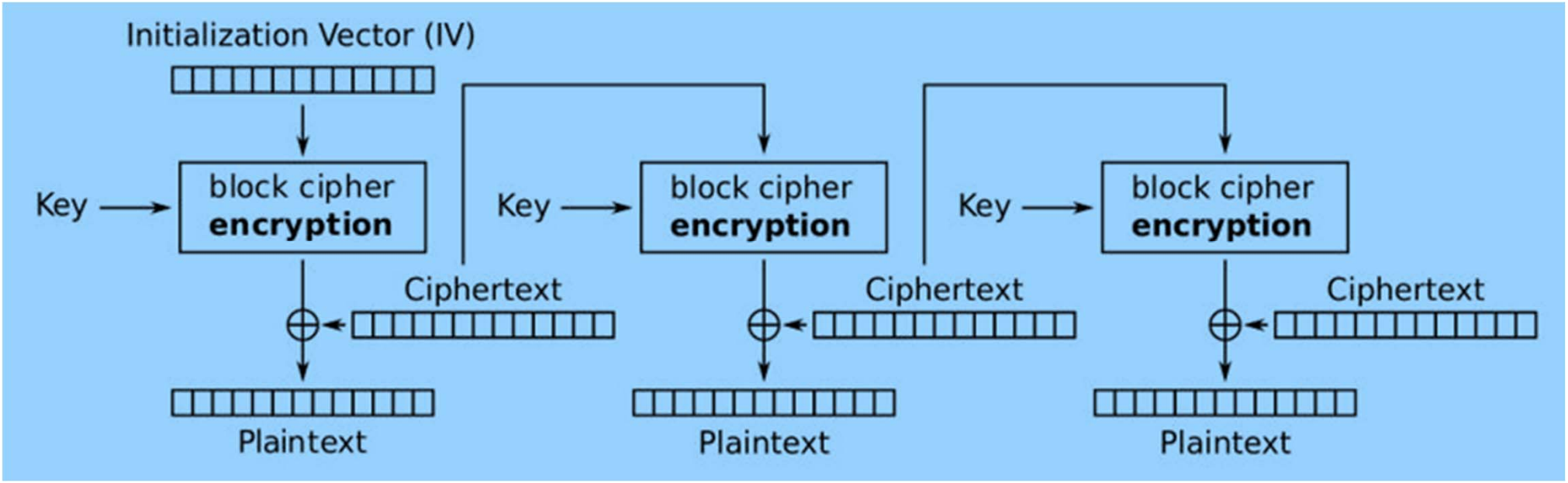


CFB Encryption

$$C_0 = E_K(IV) \oplus P_0,\ C_i = E_K(C_{i-1}) \oplus P_i,\quad P_i = E_K(C_{i-1}) \oplus C_i,$$

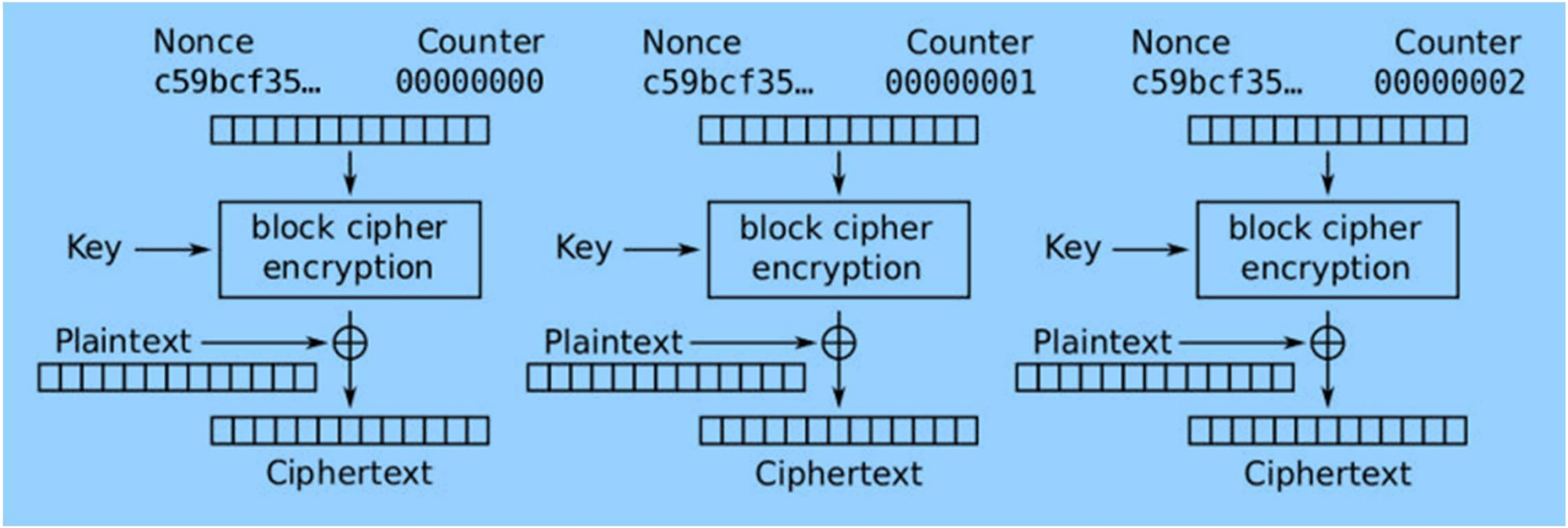


CFB Decryption

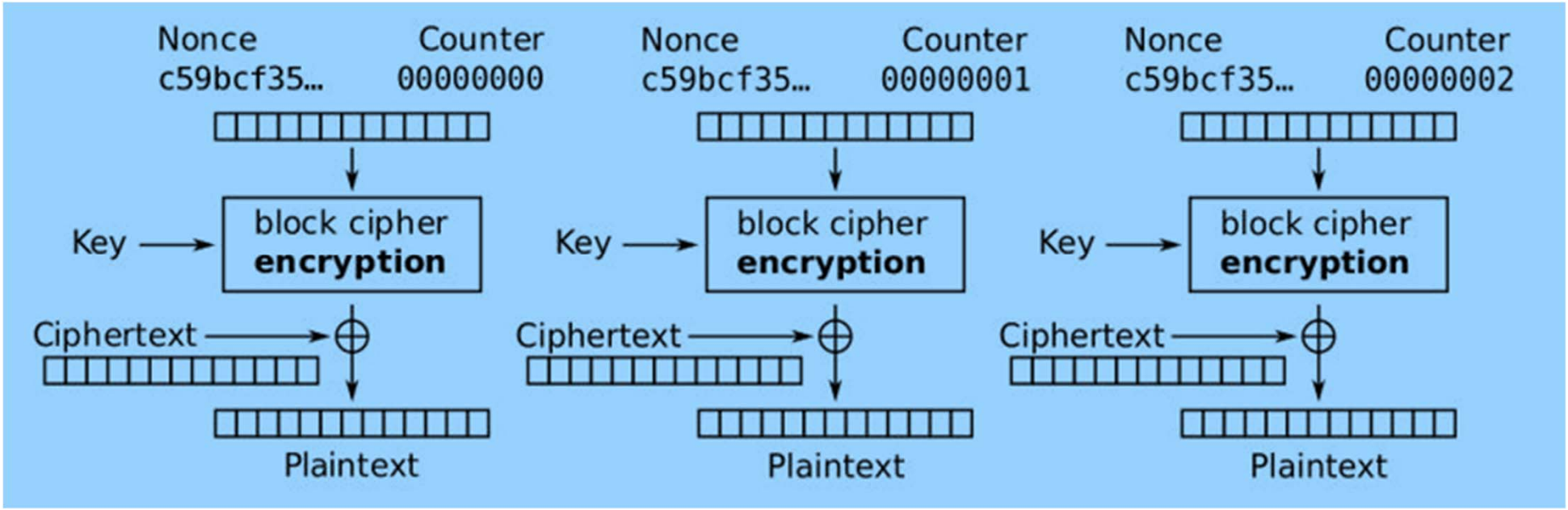


CTR Encryption

$C_i = E_K(IV \,||\, CTR_i) \oplus P_i$, $P_i = E_K(IV \,||\, CTR_i) \oplus C_i$,…



CTR Decryption



Advantage of CTR

- The encryption/decryption of all blocks can be processed in parallel.

Question

- Why are there so many modes operations? Which one can be recommended for your use?
- IV should be nonce. How can we generate IVs every time new message blocks are sent?
- In doing this block operation, at the same time can we do the integrity and authentication check of the message?
  - i.e., can we verify that (1) the message is really created by Alice, and (2) the ciphertext was not tampered during transmission?