Chapter 6
Block Cipher Operation

→

정보보안

Abridged version

Modes of Operation

- Motivation
  - A block cipher by itself is only suitable for the encryption of one fixed-length block.
  - A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block.

DES - 64bit block cyper

AES - 128 bit block cyper

ECB (Electronic Code Book)

- Encryption
  - $C_j = E(K, P_j)$

    for $j = 1, \ldots, N$

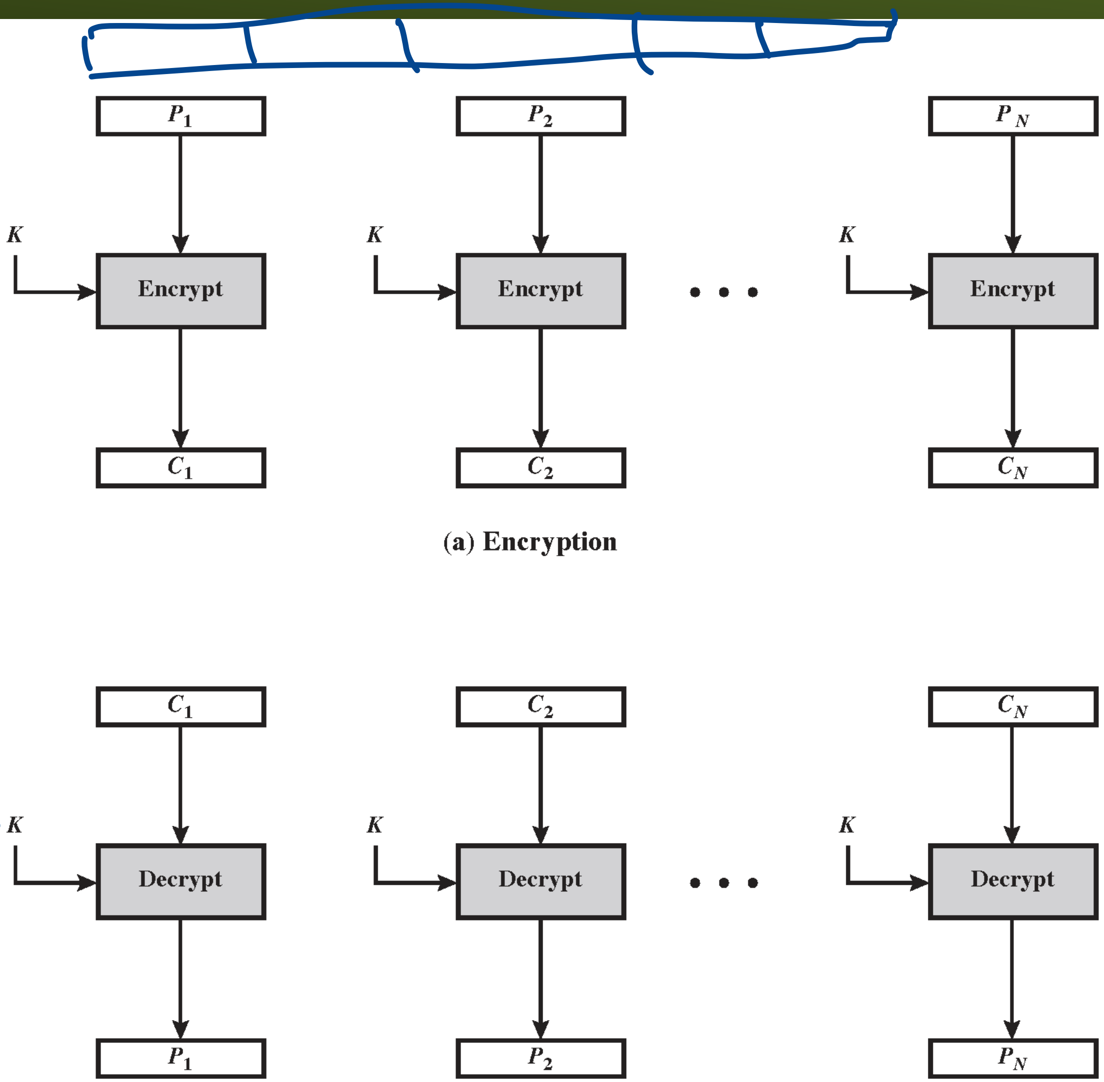
rand 숫자. 매번 바꿔야함

- Decryption
  - $P_j = D(K, C_j)$

    for $j = 1, \ldots, N$

전자 코드책

electronic code book ECB

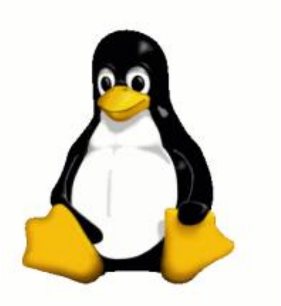


(a) Encryption

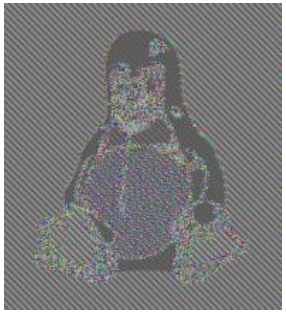
(b) Decryption

Disadvantage of ECB

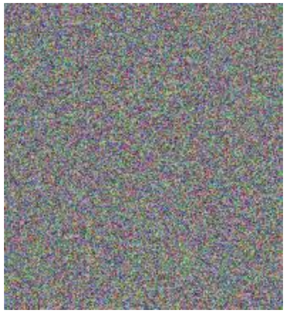
- ECB is deterministic. - 랜덤넘버가 들어가지 않음
  - The disadvantage of ECB is that identical plaintext blocks are encrypted into identical ciphertext blocks.
  - A striking example of the degree to which ECB can leave plaintext data patterns in the ciphertext can be seen when ECB mode is used to encrypt a bitmap image which uses large areas of uniform color.



Original Image



Encrypted using ECB mode



Encrypted using other modes

누가 같은 걸 썼는지 알 수 있다.

IV (Initialization Vector)

초기화해주는 vector

- Motivation
  - An initialization vector (IV) is a block of bits that is used by several modes to randomize the encryption and hence to produce distinct ciphertexts even if the same plaintext is encrypted multiple times.
- Security requirements 동일한 메시지가 들어와도 매번 랜덤.
  - The IV does not need to be secret.
  - An initialization vector is never reused under the same key.
  - In CBC mode, the IV must, in addition, be unpredictable at encryption time.

IV는 비밀일 필요 X , 매번 바뀌고, 반복해서 사용하면 안된다.

CBC (Cipher Block Chaining)

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

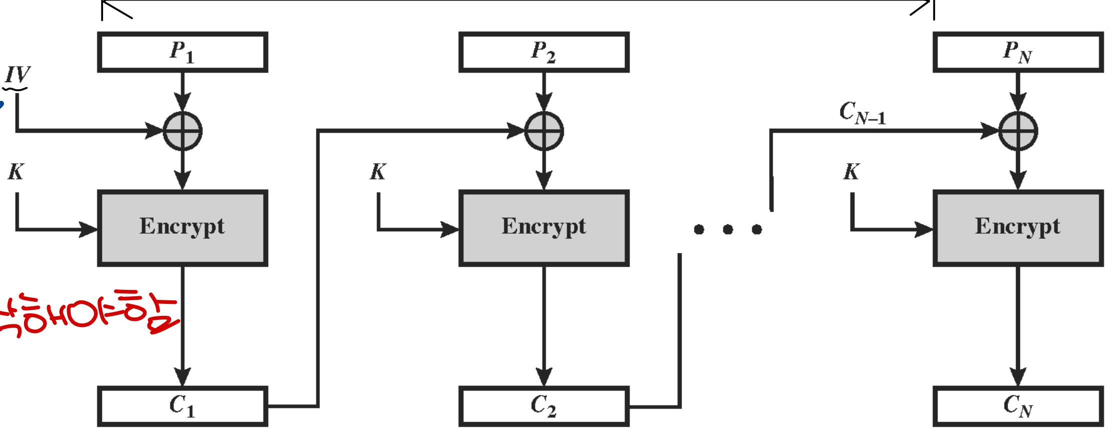
중간에 오류나면 소용X. 다시 시작해야함

처음만 IV를 뽑고, C1을 사용

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

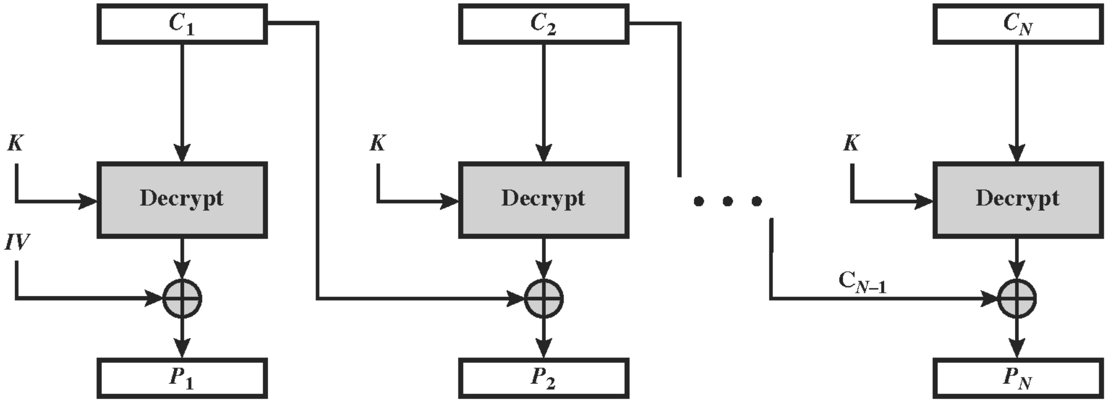
AES라면 128 bit 이므로
IV도 128bit

영화 한편. 10G P면 IV도 10G need. 총 20G, 첫번째만 IV를 새로 뽑고, C_1을 IV인것처럼 사용



(a) Encryption

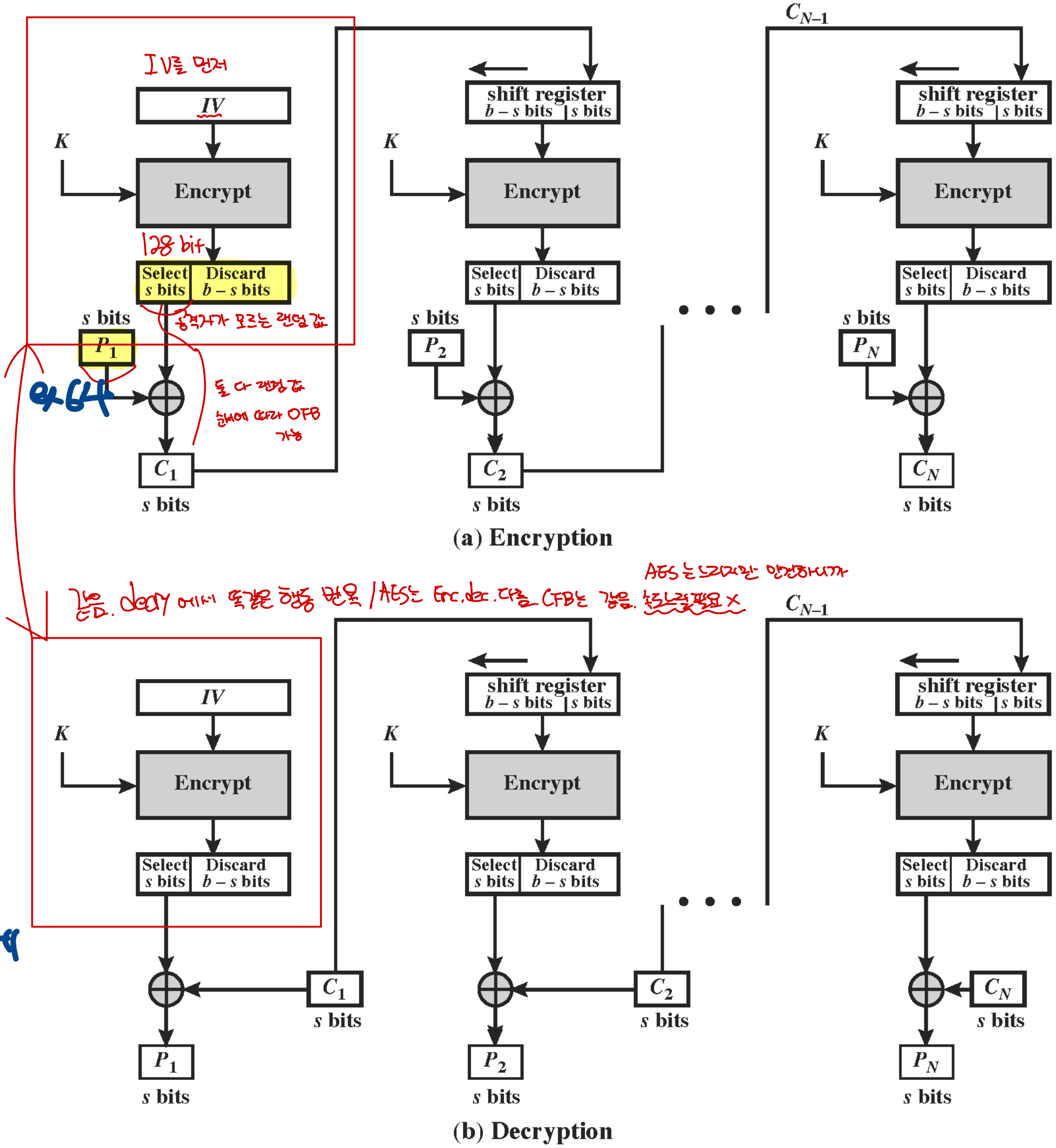
같다 128 bit



(b) Decryption

CFB (Cipher Feedback)

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

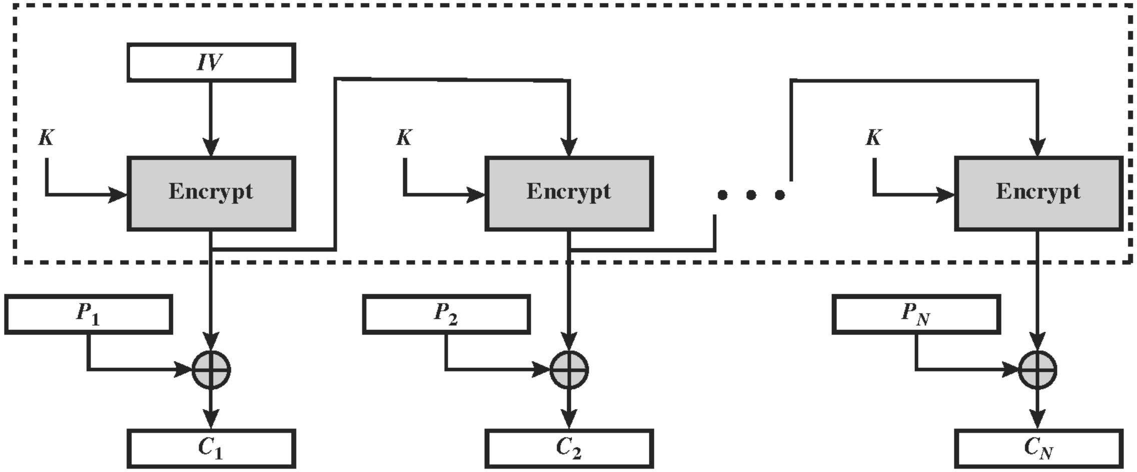


AES
Mix column 에서 행렬 때문에
속도가 느림
decry는 역함수가-보다 복잡

OFB (Output Feedback)

- Encryption
  - $I_0 = IV$
  - $I_j = O_{j-1}$
  - $O_j = E(K, I_j)$
  - $C_j = P_j \oplus O_j$
- Decryption
  - $I_0 = IV$
  - $I_j = O_{j-1}$
  - $O_j = E(K, I_j)$
  - $P_j = C_j \oplus O_j$

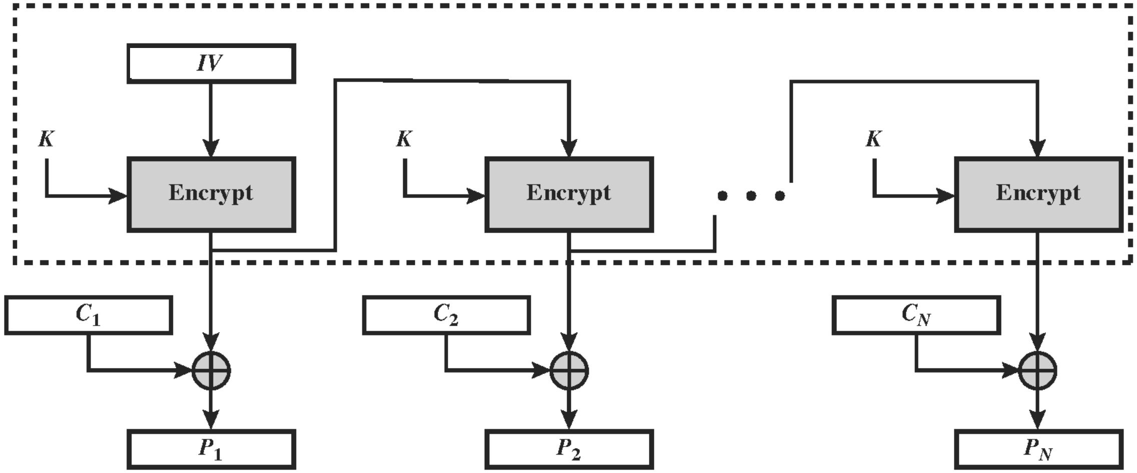
점선부분 메세지와 상관 없음. 미리 계산해놓고, 메시지가 올때 XOR만 해서 보냄



한비트가 오류나도 오류난 그것만 다시.

(a) Encryption

사전계산 가능

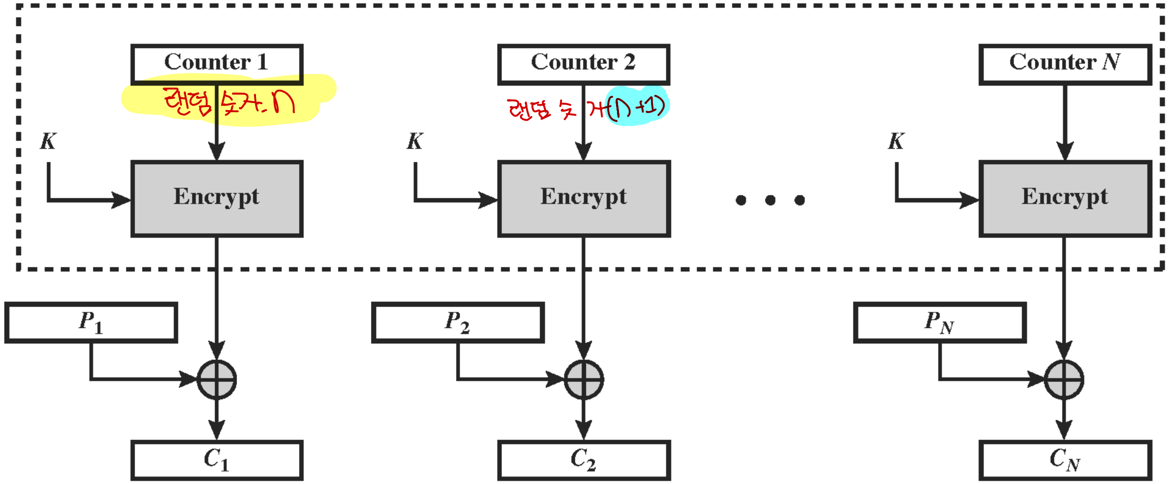


(b) Decryption

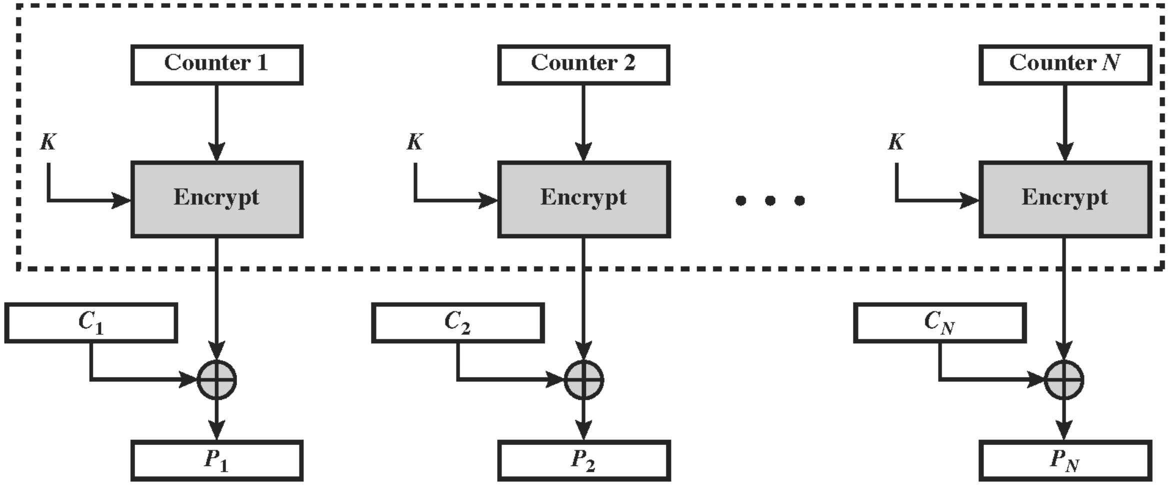
CTR (Counter)

일 분배 가능 . 제일 뒤쪽부터 작업 가능

- Encryption
  - $C_j = P_j \oplus E(K, T_j)$
- Decryption
  - $P_j = C_j \oplus E(K, T_j)$



(a) Encryption



(b) Decryption

Characteristics

- CFB, OFB, CTR ~~ECB~~ 안전X
  - The block cipher is only used in the encryption direction.
- OFB, CTR
  - Bit errors in transmission do not propagate.
  - The block cipher operations may be performed in advance.
- CTR
  - The *i*th block of plaintext or ciphertext can be processed in random-access fashion.
  - CTR mode is well suited to operate on a multi-processor machine where blocks can be encrypted/decrypted in parallel.

병렬처리가능

NIST Block Cipher Modes

- 8 confidentiality modes
  - ECB, CBC, OFB, CFB, CTR, XTS-AES, FF1, FF3.
- 1 authentication mode
  - CMAC BLOCK Ciper 인증하기 위한 제대로된것 : CMAC
- 5 combined modes for confidentiality and authentication
  - CCM, GCM, KW, KWP, TKW