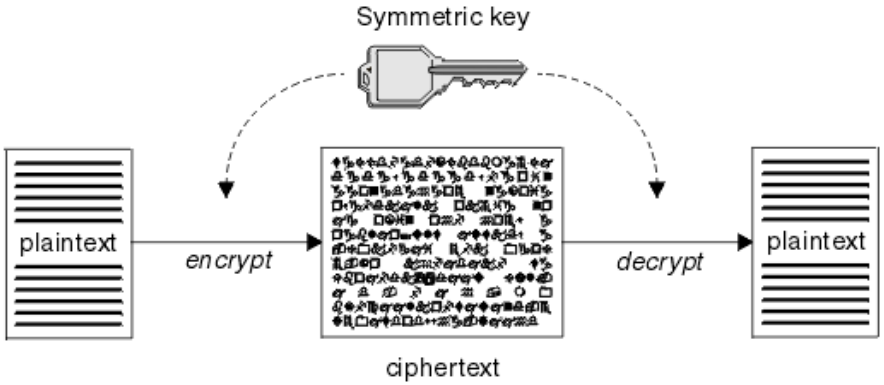


Computer Security

Symmetric Encryption

If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees.
—Kahlil Gibran

Tamer ABUHMED
Department of Computer Science & Engineering
Sungkyunkwan University

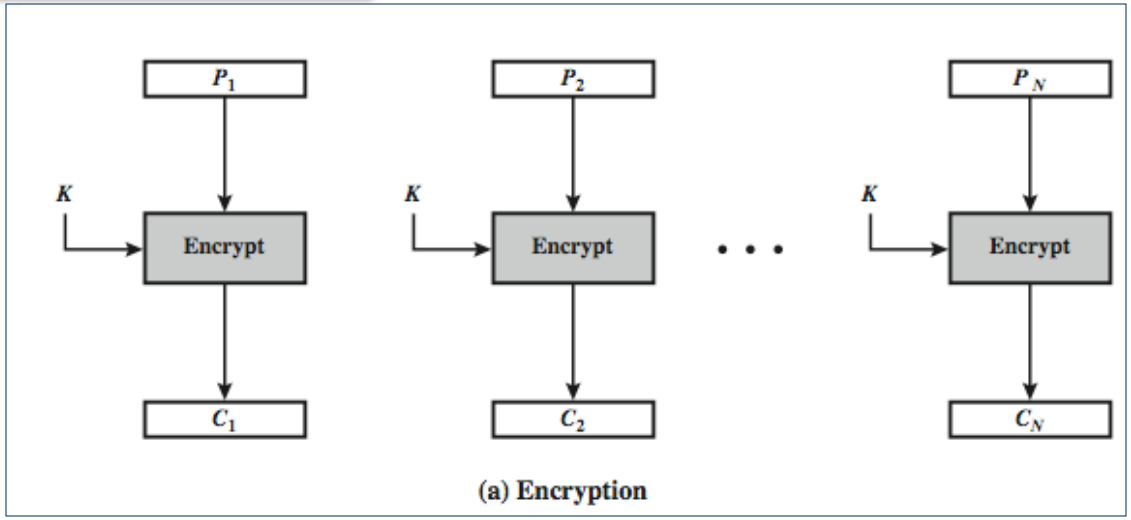
SUNG KYUN KWAN UNIVERSITY

Modes of Operations

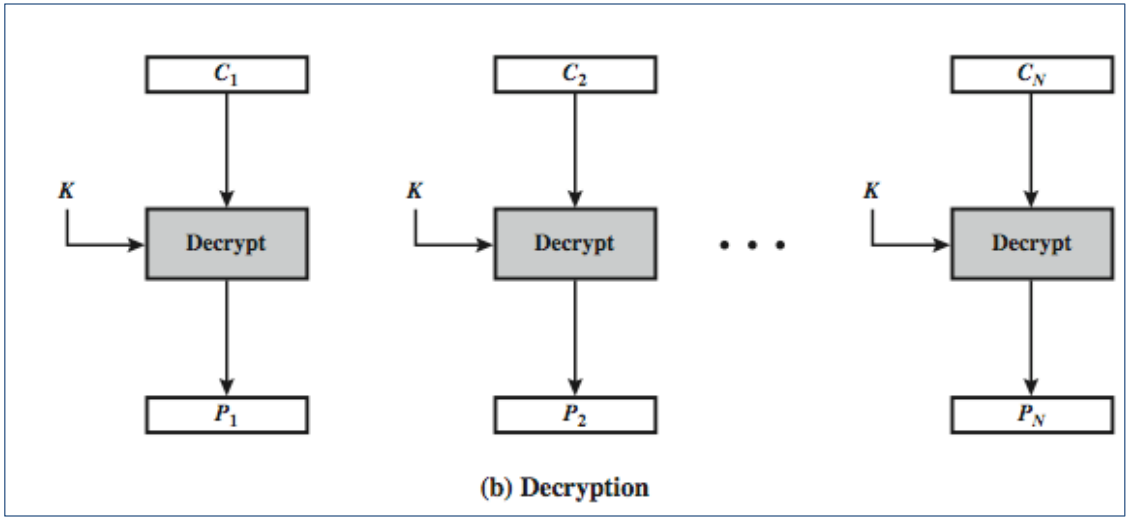
- block ciphers encrypt fixed size blocks
  - DES and 3DES encrypt 64-bit blocks
  - AES uses 128-bit blocks
- in practise, we have arbitrary amount of information to encrypt
  - we use DES, 3DES, AES and other symmetric ciphers in different modes in order to apply to several data blocks
- NIST SP 800-38A defines 5 modes
  - can be used with any block cipher

Electronic Codebook (ECB) Mode

- each block is encrypted independent of the other blocks
  - using the same key
- not so secure for long messages due to repetitions in code



(a) Encryption



(b) Decryption

ECB Mode

- Notation: C = E(P,K)
- Given plaintext $P_0,P_1,\ldots,P_m,\ldots$
- Most obvious way to use a block cipher:

Encrypt	**Decrypt**
$C_0 = E(P_0, K)$	$P_0 = D(C_0, K)$
$C_1 = E(P_1, K)$	$P_1 = D(C_1, K)$
$C_2 = E(P_2, K)$ …	$P_2 = D(C_2, K)$ …

- For fixed key K, this is "electronic" version of a codebook cipher (without additive)
  - With a different codebook for each key

ECB Cut and Paste

- Suppose plaintext is

  `Alice digs Bob. Trudy digs Tom.`

- Assuming 64-bit blocks and 8-bit ASCII:

  P_0 = "`Alice di`", P_1 = "`gs Bob. `",

  P_2 = "`Trudy di`", P_3 = "`gs Tom. `"

- Ciphertext: C_0, C_1, C_2, C_3
- Trudy cuts and pastes: C_0, C_3, C_2, C_1
- Decrypts as

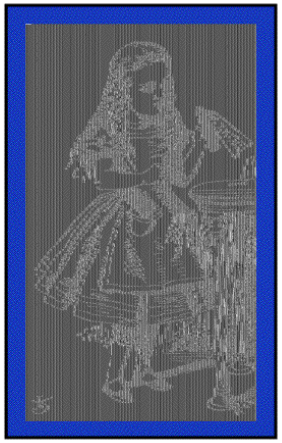
  `Alice digs Tom. Trudy digs Bob.`

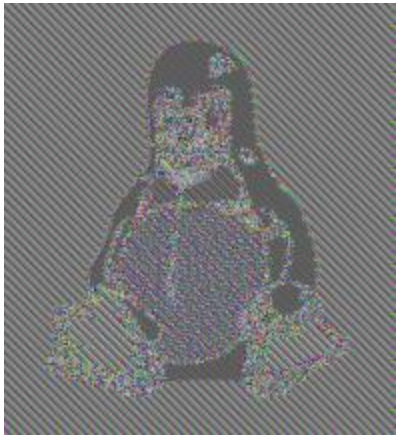
ECB Weakness

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

Alice Hates ECB Mode

- Alice's uncompressed image, and ECB encrypted

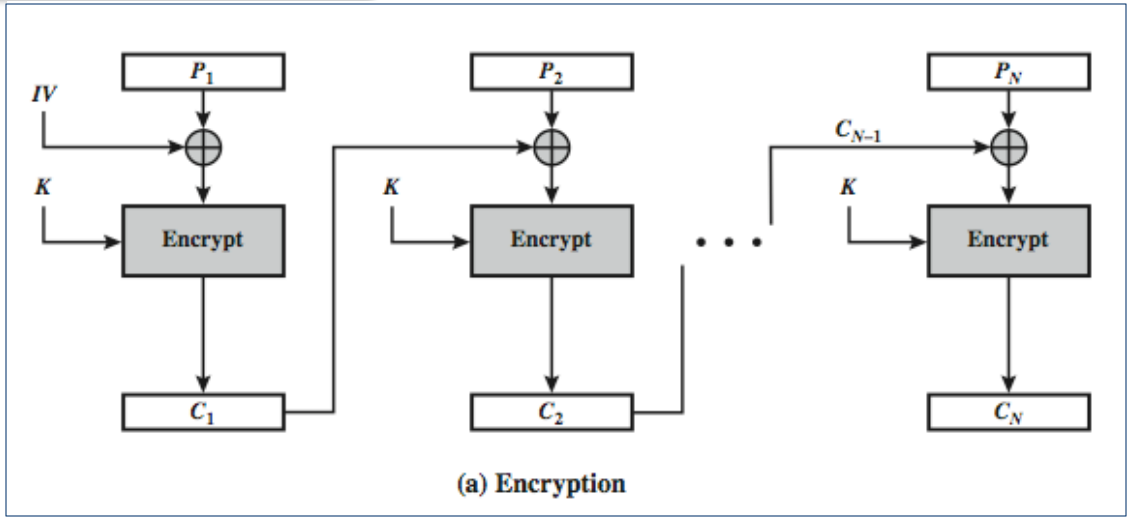



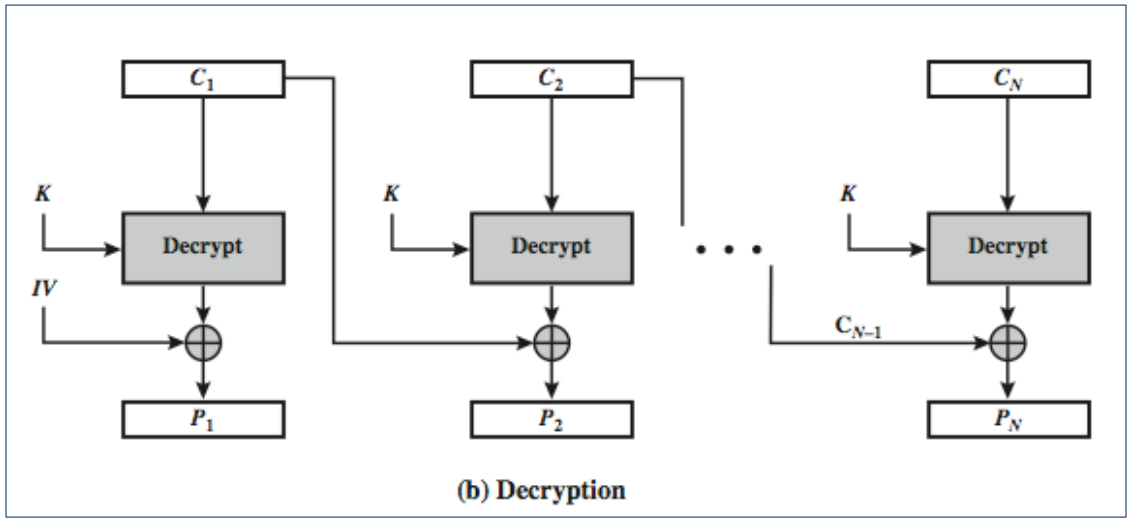


- Why does this happen?
- Same plaintext yields same ciphertext!

Cipher Block Chaining (CBC)

- each previous cipher blocks is XORed with current plaintext
- each ciphertext block depends on all previous blocks
- need Initialization Vector (IV) known to sender & receiver



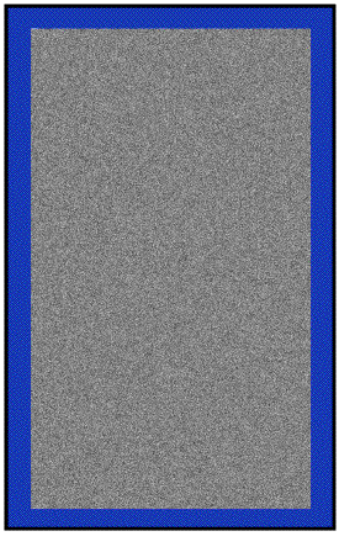


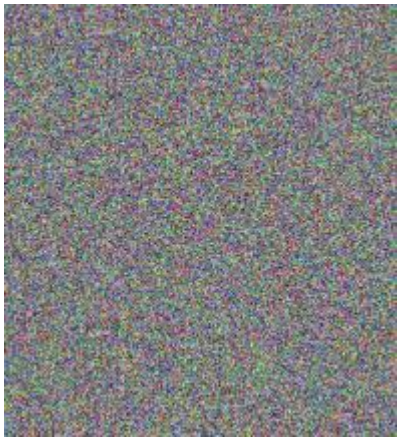
Cipher Block Chaining (CBC)

- Initialization Vector (IV)
  - both parties should agree on an IV
  - for maximum security, IV should be protected for unauthorized changes
  - Otherwise, attacker's change in IV also changes the decrypted plaintext
    - let's see this on board

Alice Likes CBC Mode

- Alice's uncompressed image, Alice CBC encrypted

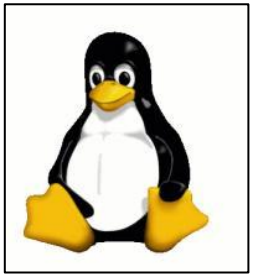


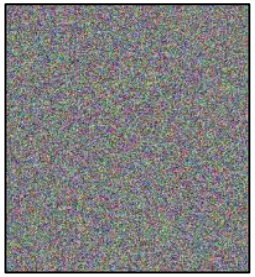
- Why does this happen?
- Same plaintext yields different ciphertext!

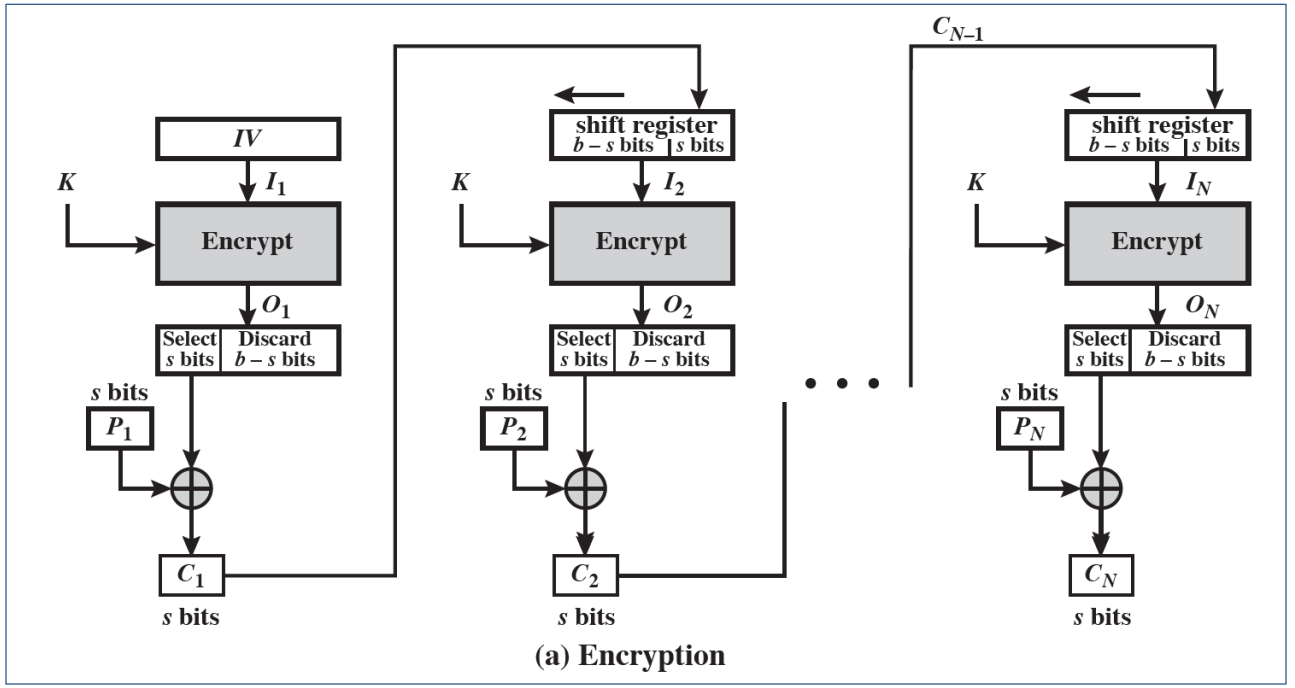
Cipher FeedBack (CFB)

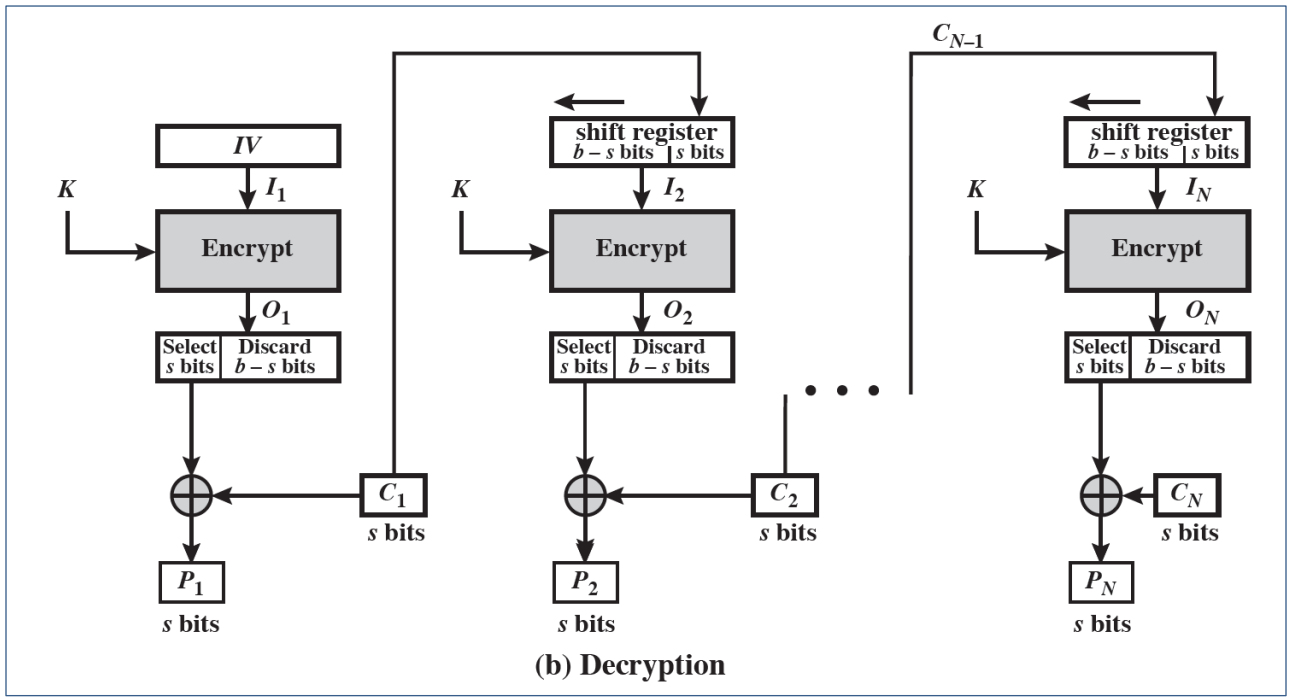
- Message is treated as a stream of bits
  - DES, AES (or any other block cipher) is used as a stream cipher
- standard allows any number of bit, *s*, (1,8 or more until the block size) as the unit of encryption/decryption
  - But common value for *s* is 8.
  - Plaintext is divided into block of *s* bits.
- uses IV
  - as all other stream ciphers
- Result of encryption is fed back to the next stage
- transmission errors propagate

Cipher FeedBack (CFB) Mode





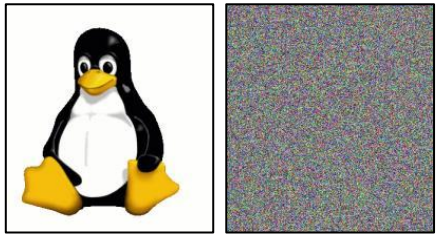


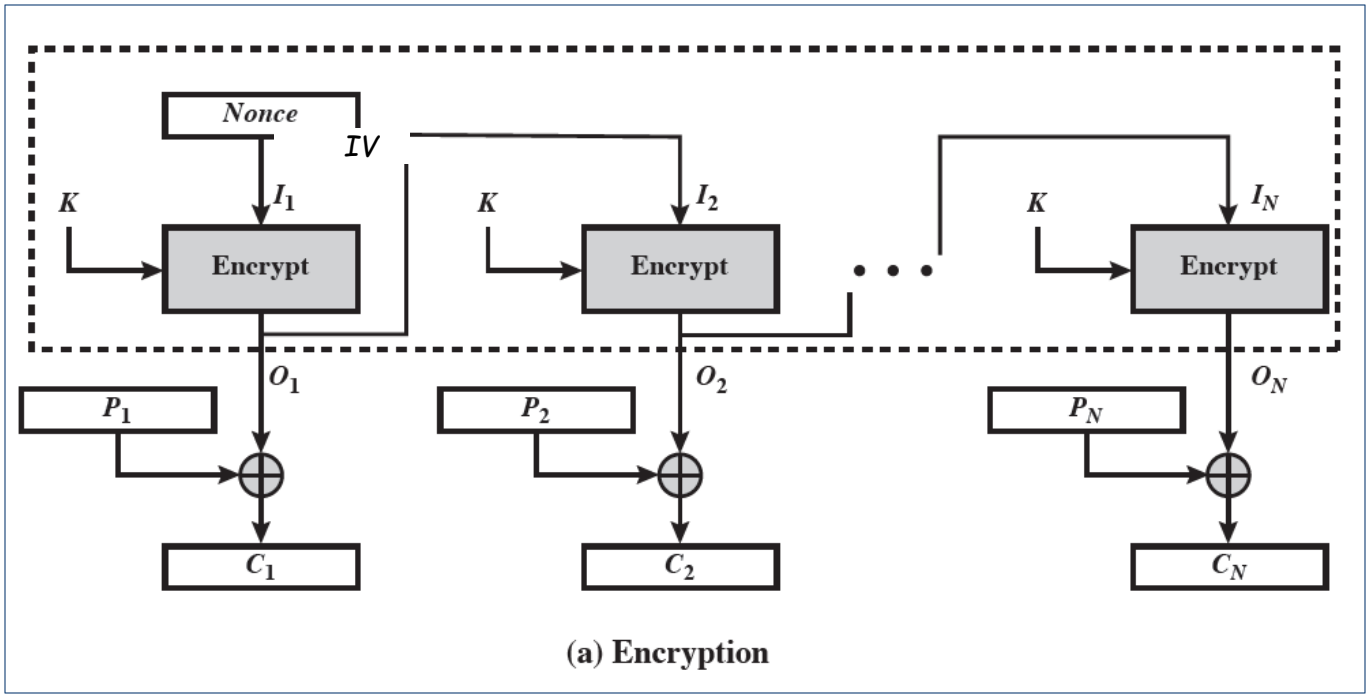


Output FeedBack (OFB)

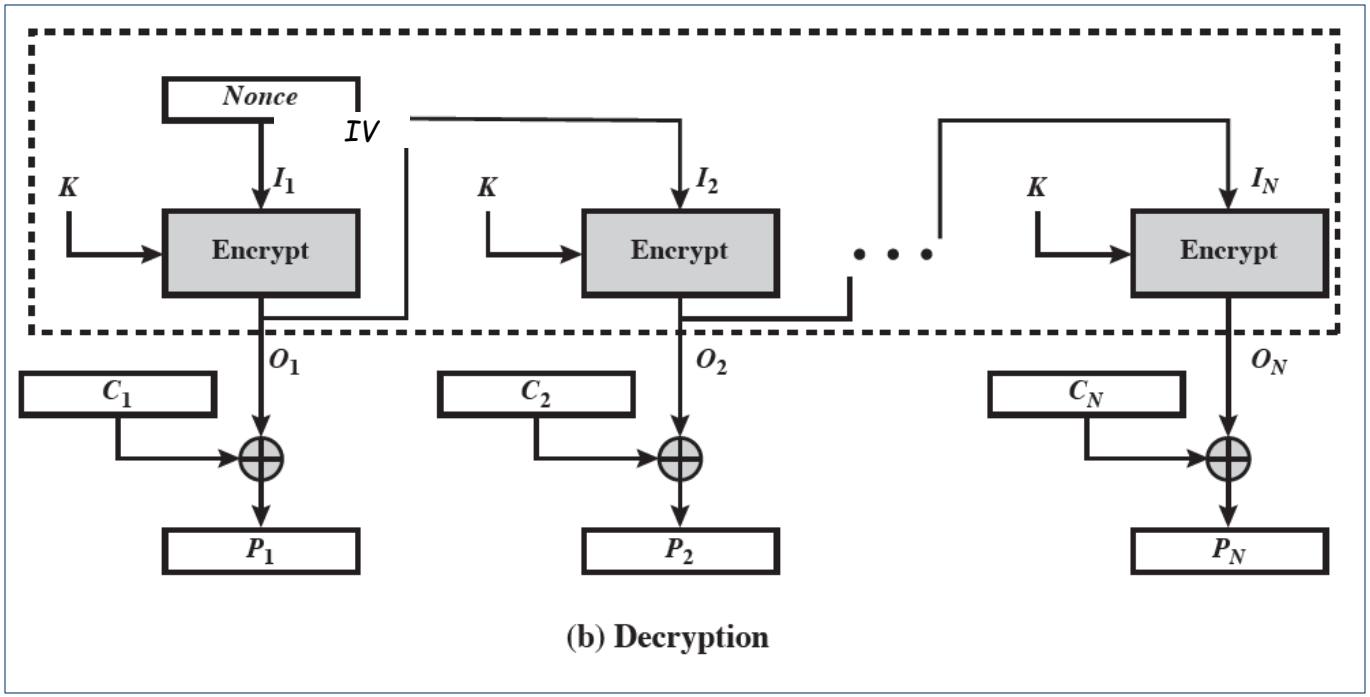
- another stream mode
  - but, *s*-bit version does not exist anymore
    - Full block is used in the encyption and decryption
- output of cipher is
  - XORed with the message
  - it is also the feedback
- feedback is independent of transmission, so transmission errors do not propagate
- same IV should not be used twice for the same key (general problem of using IV)
  - otherwise, when two ciphertext blocks are XORed the random sequence is cancelled and the attacker obtains XOR of two plaintexts
  - That is why IV is sometimes called as *nonce* (means "*used only once*")

Output FeedBack (OFB)





(a) Encryption

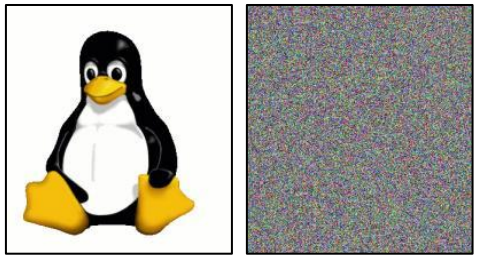


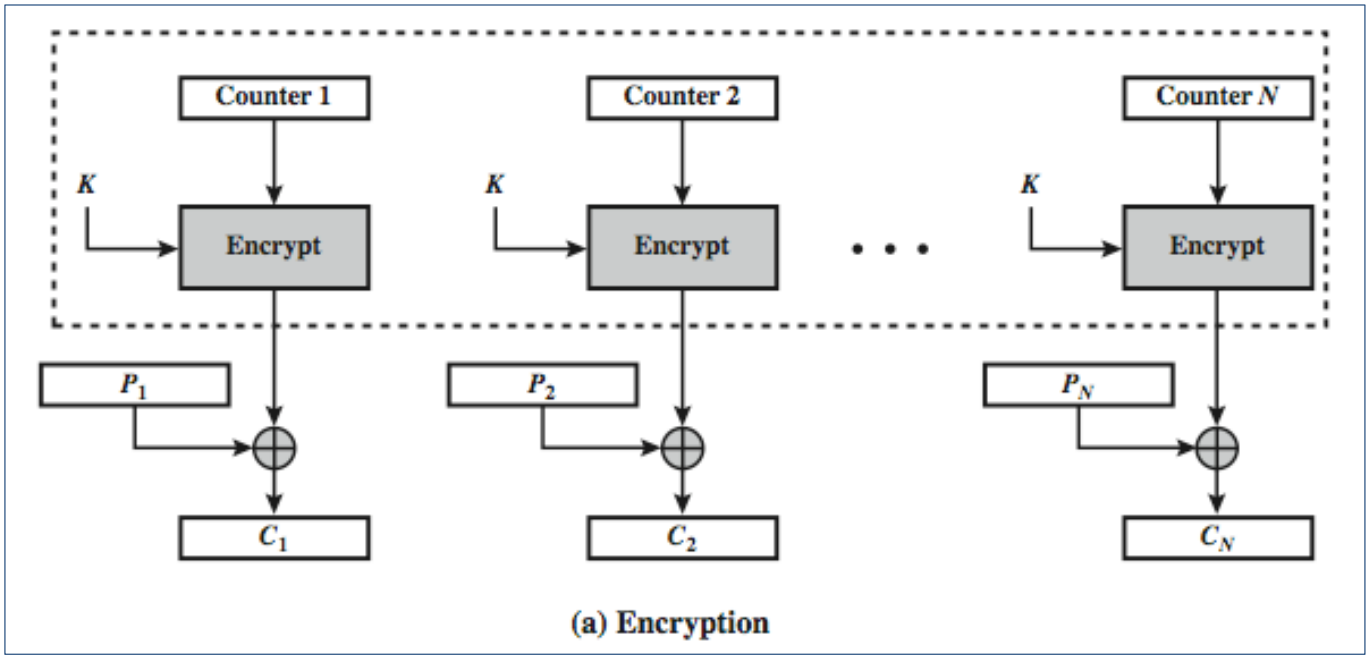
(b) Decryption

Counter (CTR)

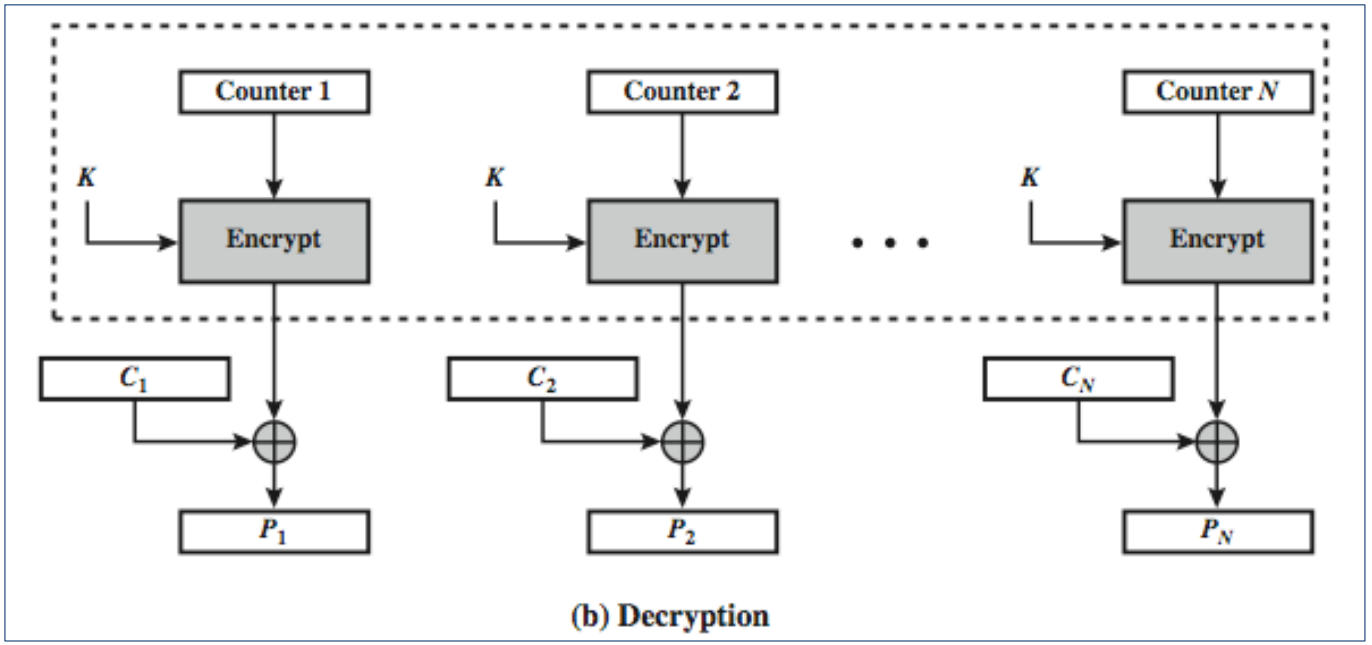
- similar to OFB but encrypts counter value rather than any feedback value
- For the same key, the counter value should not repeat
  - same problem as in OFB
- efficient
  - can do parallel encryptions
  - Cryptographic part of the process (encryption blocks) is performed in advance of need
  - good for bursty high speed links

Counter (CTR)





(a) Encryption



(b) Decryption