Chapter 3 Block Ciphers and the Data Encryption Standard

Cryptography and Network Security:
Principles and Practices (3rd Ed.)

3.2 Block Cipher Principle

- Block vs Stream Ciphers
  - block ciphers process messages in into *blocks, each of which is then en/decrypted*.
  - like a substitution on very big characters
    - 64-bits or more.
  - stream ciphers process messages *a bit or byte at a time when en/decrypting*.
  - many current ciphers are block ciphers.
  - hence are focus of course.

3.7 Block Cipher Modes of Operation

- Modes of Operation
  - block ciphers encrypt fixed size blocks.
  - eg. DES encrypts 64-bit blocks, with 56-bit key
  - need way to use in practise, given usually have arbitrary amount of information to encrypt.
  - four were defined for DES in ANSI standard **ANSI X3.106-1983 Modes of Use**.
  - subsequently now have 5 for DES and AES.
  - have **block** and **stream** modes.

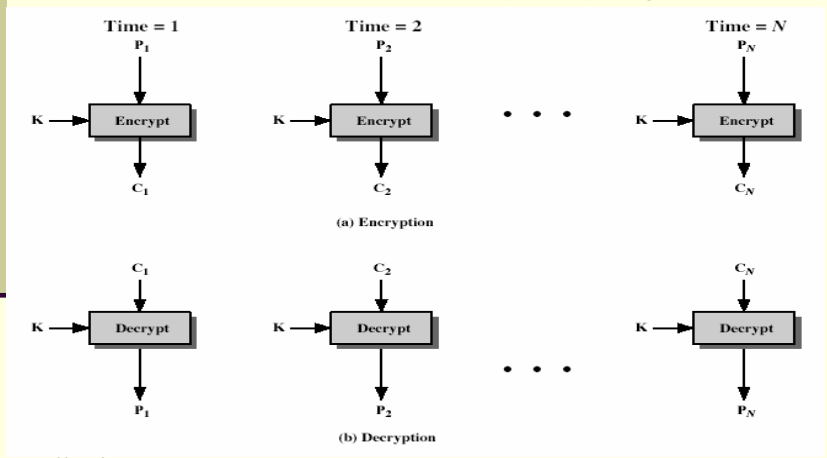
3.7 Block Cipher Modes of Operation

- Electronic Codebook Book (ECB)
  - message is broken into independent blocks which are encrypted.
  - each block is a value which is substituted, like a codebook, hence name.
  - each block is encoded independently of the other blocks

    $C_i = DES_{K1}(P_i)$
  - uses: secure transmission of single values.

3.7 Block Cipher Modes of Operation

- Electronic Codebook Book (ECB)[Fig. 3.11]



5

3.7 Block Cipher Modes of Operation

- Advantages and Limitations of ECB
  - repetitions in message may show in ciphertext
    - if aligned with message block
    - particularly with data such graphics
    - or with messages that change very little, which become a code-book analysis problem
  - weakness due to encrypted message blocks being independent
  - main use is sending a few blocks of data.

3.7 Block Cipher Modes of Operation

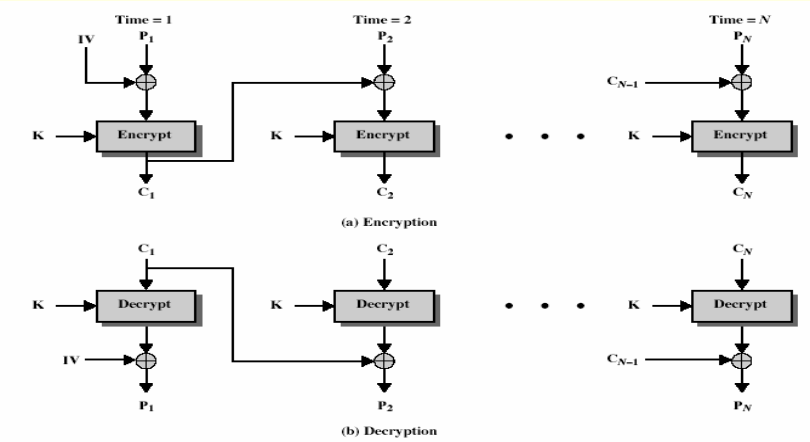
- Cipher Block Chaining (CBC)
  - message is broken into blocks
  - but these are linked together in the encryption operation
  - each previous cipher blocks is chained with current plaintext block, hence name
  - use Initial Vector (IV) to start process

    $C_i = DES_{K1}(P_i \text{ XOR } C_{i-1})$

    $C_{-1} = IV$
  - uses: bulk data encryption, authentication

3.7 Block Cipher Modes of Operation

- CBC [Fig. 3.12]



3.7 Block Cipher Modes of Operation

- Advantages and Limitations of CBC
  - each ciphertext block depends on **all** message blocks
  - thus a change in the message affects all ciphertext blocks after the change as well as the original block
  - need **Initial Value** (IV) known to sender & receiver
    - however if IV is sent in the clear, an attacker can change bits of the first block, and change IV to compensate
    - hence either IV must be a fixed value (as in EFTPOS) or it must be sent encrypted in ECB mode before rest of message
  - at end of message, handle possible last short block
    - by padding either with known non-data value (eg nulls)
    - or pad last block with count of pad size
      - eg. [b1 b2 b3 0 0 0 0 5] <- 3 data bytes, then 5 bytes pad+count .

3.7 Block Cipher Modes of Operation

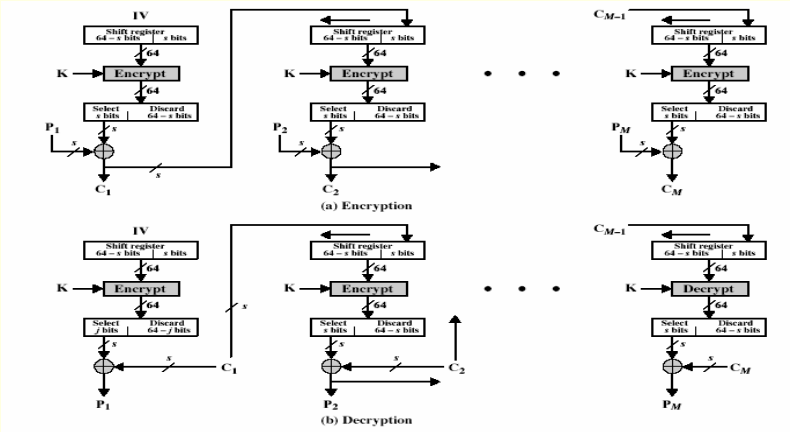
- Cipher FeedBack (CFB)
  - message is treated as a stream of bits
  - added to the output of the block cipher
  - result is feed back for next stage (hence name)
  - standard allows any number of bit (1,8 or 64 or whatever) to be feed back
    - denoted CFB-1, CFB-8, CFB-64 etc
  - is most efficient to use all 64 bits (CFB-64)

    $C_i = P_i \text{ XOR } DES_{K1}(C_{i-1})$

    $C_{-1} = IV$
  - uses: stream data encryption, authentication.

3.7 Block Cipher Modes of Operation

- CFB [Fig. 3.13]



3.7 Block Cipher Modes of Operation

- Advantages and Limitations of CFB
  - appropriate when data arrives in bits/bytes
  - most common stream mode
  - limitation is need to stall while do block encryption after every n-bits
  - note that the block cipher is used in **encryption** mode at **both** ends
  - errors propagate for several blocks after the error.

3.7 Block Cipher Modes of Operation

- Output FeedBack (OFB)
  - message is treated as a stream of bits
  - output of cipher is added to message
  - output is then feed back (hence name)
  - feedback is independent of message
  - can be computed in advance

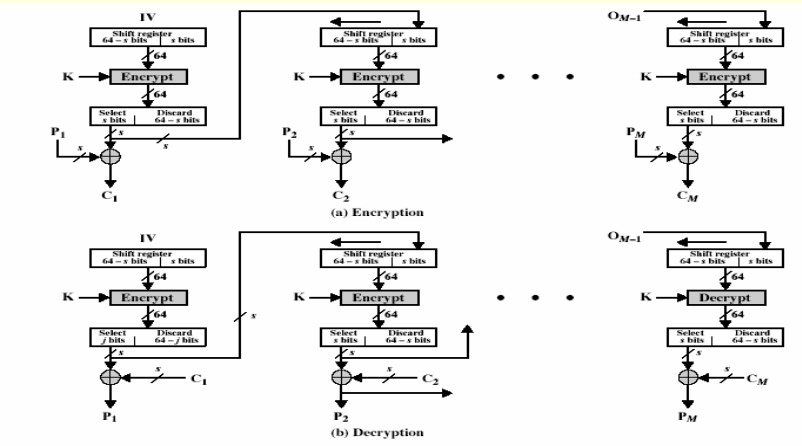
    $C_i = P_i \text{ XOR } O_i$

    $O_i = DES_{K1}(O_{i-1})$

    $O_{-1} = IV$
  - uses: stream encryption over noisy channels.

3.7 Block Cipher Modes of Operation

- OFB [Fig. 3.14]



3.7 Block Cipher Modes of Operation

- Advantages and Limitations of OFB
  - used when error feedback a problem or where need to encryptions before message is available
  - superficially similar to CFB
  - but feedback is from the output of cipher and is independent of message
  - a variation of a Vernam cipher
    - hence must **never** reuse the same sequence (key+IV)
  - sender and receiver must remain in sync, and some recovery method is needed to ensure this occurs
  - originally specified with m-bit feedback in the standards
  - subsequent research has shown that only **OFB-64** should ever be used

3.7 Block Cipher Modes of Operation

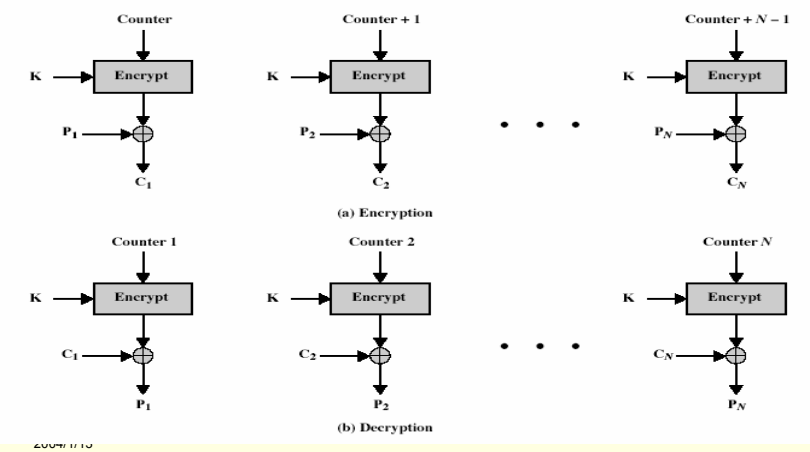
- Counter (CTR)
  - a "new" mode, though proposed early on
  - similar to OFB but encrypts counter value rather than any feedback value
  - must have a different key & counter value for every plaintext block (never reused)

    $C_i = P_i \text{ XOR } O_i$

    $O_i = DES_{K1}(i)$
  - uses: high-speed network encryptions.

3.7 Block Cipher Modes of Operation

- CTR [Fig. 3.15]



3.7 Block Cipher Modes of Operation

- Advantages and Limitations of CTR
  - efficiency
    - can do parallel encryptions
    - in advance of need
    - good for bursty high speed links
  - random access to encrypted data blocks
  - provable security (good as other modes)
  - but must ensure never reuse key/counter values, otherwise could break (cf OFB).