Arab Academy for Science Technology and Maritime Transport
College of Computing and Information Technology

Course	Computer System Security
Course Code	CS421
Lecturer	Prof. Dr Ayman Adel
TA	Maram Shouman, Menna Elmasry

Sheet 4

Review Questions: (2 marks per each question)

1. List and briefly define the block cipher modes of operation.
2. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?
3. Draw the electronic codebook mode for encryption and decryption.
4. Draw the cipher block chaining mode for encryption and decryption.
5. Draw the cipher feedback mode for encryption and decryption.
6. Draw the output feedback mode for encryption and decryption.
7. Draw the counter mode for encryption and decryption.

Problems: (5 marks per each question)

1. Can you suggest a security improvement to either option in Figure 7.17, using only three DES chips and some number of XOR functions? Assume you are still limited to two keys.

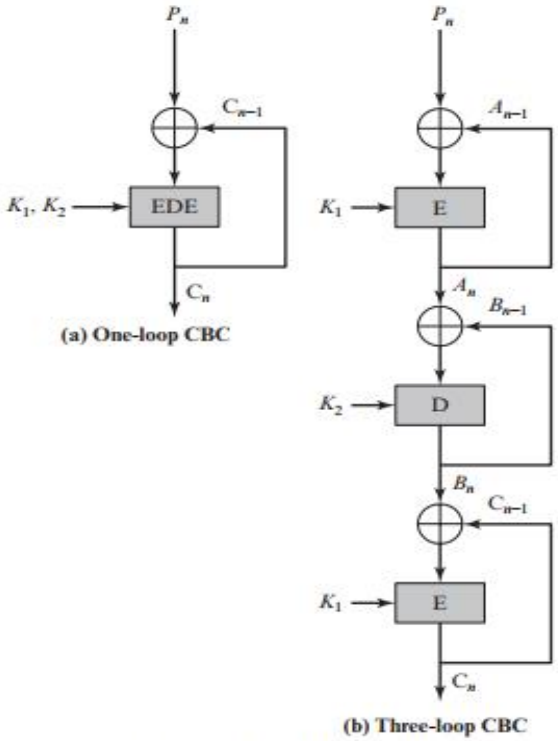

Figure 7.17 Use of Triple DES in CBC Mode

2. Is it possible to perform encryption operations in parallel on multiple blocks of plain-text in CBC mode? How about decryption?
3. For the ECB, CBC, and CFB modes, the plain-text must be a sequence of one or more complete data blocks (or, for CFB mode, data segments). In other words, for these three modes, the total number of bits in the plain-text must be a positive multiple of the block (or segment) size. One common method of padding, if needed, consists of a 1 bit followed by as few zero bits, possibly none, as are necessary to complete the final block. It is considered good practice for the sender to pad every message, including messages in which the final message block is already complete. What is the motivation for including a padding block when padding is not needed?
4. If a bit error occurs in the transmission of a cipher-text character in 8-bit CFB mode, how far does the error propagate?
5. Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? How about decryption?
6. Use Java to write an application that shows encryption and decryption using all modes of operations. State the OS time for each operation.