Tutorial 4: Cipher Block Modes

1. The ECB (Electronic Code Book) cipher mode strangely enough refers to the manner in which a cipher is attacked, not used. Describe how the ECB mode is used and how it is attacked.
2. With ECB Mode of DES, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C_1 obviously corrupts P_1 and P_2.

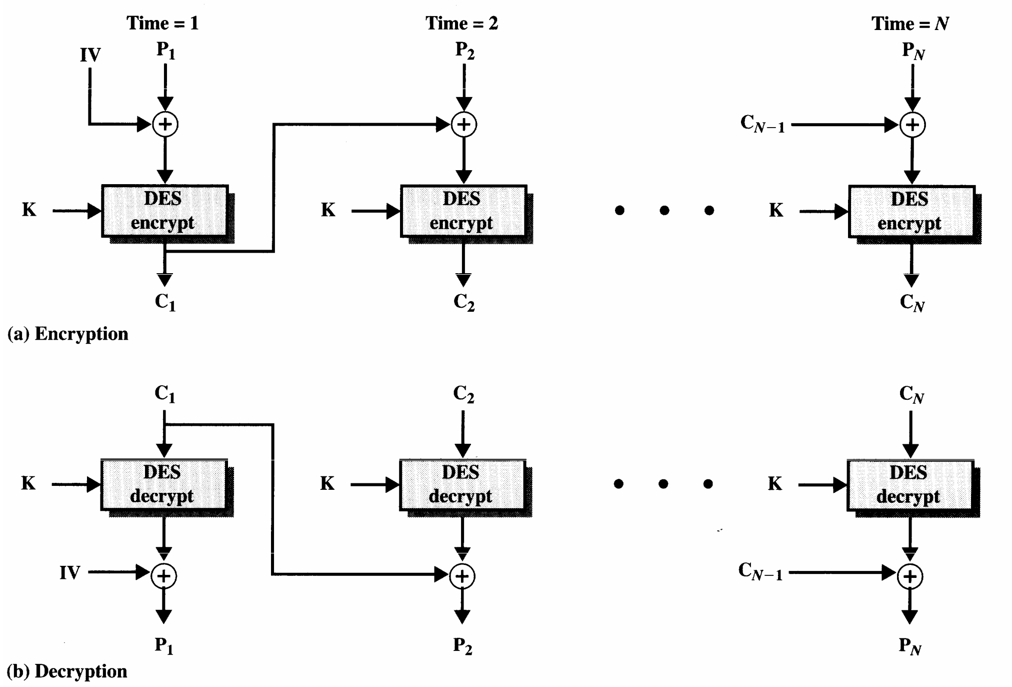

Figure 3.12 Cipher Block Chaining (CBC) Mode.

   a. Are any blocks beyond P_1 and P_2 affected?
   b. Suppose that there is a bit error in the source version of P1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?
3. If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate?
4. The enciphering of a popular cipher mode which improves the security of a cipher is OFB mode. Refer to the diagram of OFB mode in the slides:
   a. Describe the error extension and synchronization characteristics of OFB.
   b. In the diagram, the key stream k_i do not depend on the stream of ciphertext and are ideally non-repeating. In practice however they repeat at an interval which depends on the encryption algorithm used. Where IDEA is used in the algorithm, determine the maximum possible length of the sequence before it begins to repeat.
5. Explain with the aid of a sketch how a block cipher can be used with feedback or feed forward to produce non-repeating ciphertext stream, regardless of the nature of the plaintext input. Explain why such schemes are used.
6. OFB (output feedback mode) is useful in data streaming applications such as Secure Sockets Layer (SSL). Draw a block diagram showing how OFB may be implemented using a symmetric block cipher. Discuss any attack(s) which OFB mode is resistant to, what special provisions have to be made to ensure this resistance.