Lecture NS3 2018

Chapter 7

1. Compare multiple encryption/decryption schemes with the DES algorithm. What can be said regarding the strength of the encryption in each case

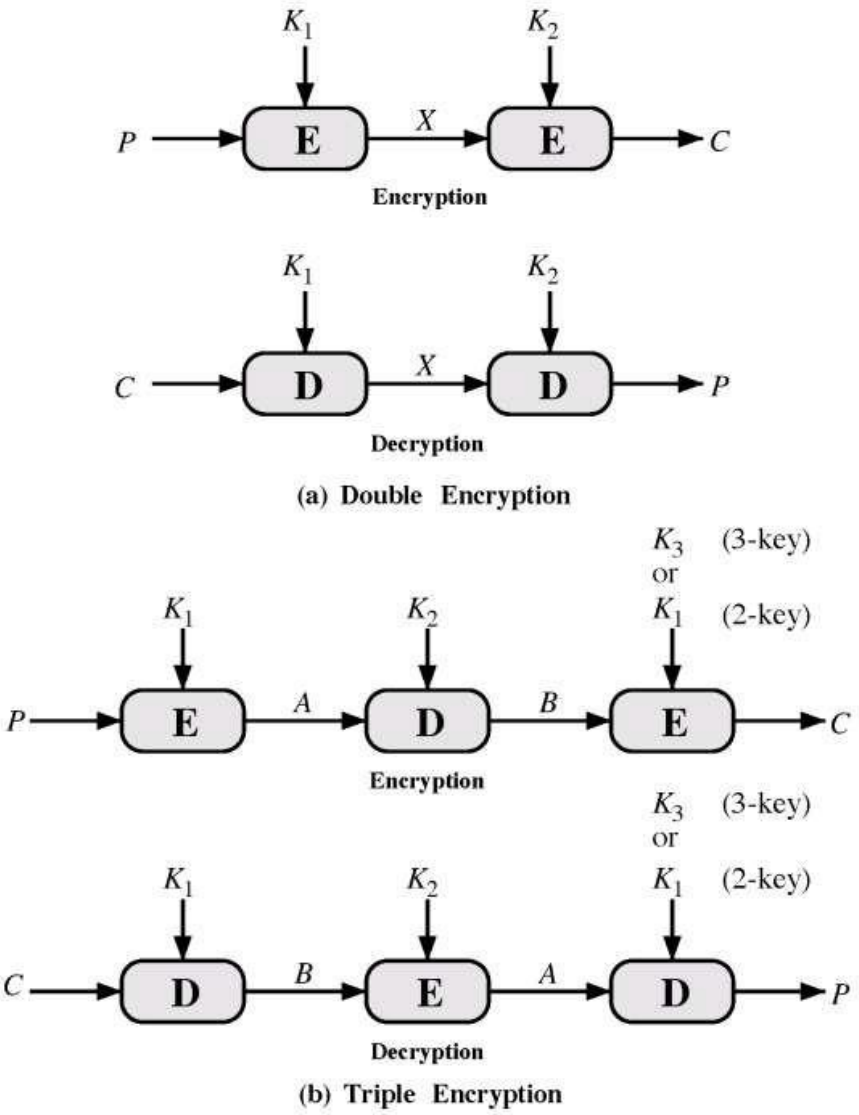

Figure 7.1 Multiple Encryption

2. Describe **the meet-in-the-middle attack** in the multiple DES encryption scheme.

   Textbook Section 7.1 (p. 210)

3. Describe five modes of operation of block ciphers.

Table 7.1 Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

4. Describe in detail Cipher Block Chaining (CBC) mode

Answer: Section 7.3

Chapter 8

5. Consider the pseudorandom number generator using the linear congruential algorithm

With the linear congruential algorithm, a choice of parameters that provides a full period does not necessarily provide a good randomization. For example, consider the following two generators:

$$X_{n+1} = (11X_n) \bmod 13$$
$$X_{n+1} = (2X_n) \bmod 13$$

Write out the two sequences to show that both are full period. Which one appears more random to you?

Answer:

Let us start with an initial seed of 1. The first generator yields the sequence:

$$1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1, \ldots$$

The second generator yields the sequence:

$$1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1, \ldots$$

Because of the patterns evident in the second half of the latter sequence, most people would consider it to be less random than the first sequence.