Cryptography

ECE 5632

Sheet 3

Spring 2024

Problem 1

An S-DES block cipher is used in the CBC mode to encrypt a 24-bits plaintext. What is the error propagation if the first bit is in error?

Problem 2

Consider the CFB mode for S-DES with $s = 4$ that is used to encrypt 16-bit plaintext data.

(a) Compute the error propagation if the 3rd bit is in error during decryption.

(b) Repeat (a) with $s = 2$.

Problem 3

Compare between CBC and ECB modes of operation of block ciphers. Your comparison must satisfy the following:

(a) Block diagrams of Encryption/Decryption for each mode.

(b) The possibility of streaming in each mode and how to achieve it.

(c) The possibility of preprocessing and random access in each mode.

(d) Error propagation and vulnerability to bit flipping attack in each mode.

Problem 4

DES is used in the CFB mode of operation with block segment ($s = 10$ bits). Compute the error propagation in bits if the first ciphertext bit is in error.

Problem 5

(a) Is the ECB mode recommended for use in practice? Explain your answer.

(b) What's the purpose of using a block cipher in CBC and CFB modes? Explain your answer.

(c) Is ECB mode equivalent to CBC with an all zeros IV? Explain your answer.

(d) Consider the CFB mode with s = n. Is it equivalent to CBC? Explain your answer.