Applied Cryptography: Homework 5

(Deadline: 3:00pm, 2022/03/23)

Justify your answers with calculations, proofs, and programs.

1. (20 points, question 4.10, page 133 of the textbook) Suppose a sequence of plaintext blocks, $x_1, \cdots, x_n$, yields the ciphertext sequence $y_1, \cdots, y_n$. Suppose that one ciphertext block, say y_i, is transmitted incorrectly (i.e., some 1's are changed to 0's and vice versa). Show that the number of plaintext blocks that will be decrypted incorrectly is equal to one if ECB or OFB modes are used for encryption; and equal to two if CBC or CFB modes are used.

2. (30 points, question 5.1, page 178 of the textbook) Define a toy hash function $h : (\mathbb{Z}_2)^7 \to (\mathbb{Z}_2)^4$ by the rule $h(x) = xA$ where all operations are modulo 2 and

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

   Find all preimages of $(0, 1, 0, 1)$.