COMP90043: Cryptography and security
Week 4: Workshop Questions

Preparation:

(1) Please read the file OneTimePad.pdf uploaded to Week 3 document area.

(2) Please read the notes on modes of using block cipher.

Questions: Part A

(1) Consider an experiment of a random throw of a pair of dice as discussed in the lecture. The outcome of the experiment can be modeled as a random variable R defined on the set given by

$$R = \{1, 2, 3, 4, 5, 6\} \times \{1, 2, 3, 4, 5, 6\}.$$

Consider a uniform probability distribution for the outcome so that $Pr[(i, j)] = 1/36$, for all (i, j) belonging to the set.

(a) Now consider the events formed by the sum of the two dice. Let S_j be the event when the sum of two dice is j. How many such events are possible in the experiment and determine the probability of each event.

(b) Now consider a new random variable, X, obtained by the sum of the two dice in the above experiment. Let Y be a random variable which takes a value of D if the two dice are same and N otherwise. Determine all the joint and conditional probabilities, $Pr[x, y], Pr[x \mid y]$ and $Pr[y|x]$, where $x \in \mathcal{X}$ (set consisting all possible sums) and $y \in \mathcal{Y} = \{D, N\}$.

(2) State the condition for perfect secrecy.

(3) Let C_1 and C_2 are two n bit ciphertexts obtained by encrypting using one-time pad key K on plaintexts M_1 and M_2 respectively. Show that $M_1 \oplus M_2 = C_1 \oplus C_2$. What is the consequence of Chosen Plaintext attack on the one-time pad encryption?

Questions: Part B: Block Cipher Modes

(1) If a bit error occurs in the transmission of a ciphertext character in OFB mode, how far does the error propagate? (Question 6.8)

(2) In discussing OFB, it was mentioned that if it was known that two different messages had an identical block of plaintext in the

identical position, it is possible to recover the corresponding Oi block? (Question 6.9)

(3) Why do some block cipher modes of operations only use encryption while others use both encryption and decryption? (Question 6.5)

(4) Question 6.1 and 6.2 (see below)

Part C: Homework

The following are a list of questions for students to attempt at home to get a better grasp of the concepts discussed during the workshop.

(1) What is reversible mapping? What is irreversible mapping? Think about why Fiestels algorithm works for any function F, even for the irreversible ones.

(2) What is the difference between a block cipher and a stream cipher?

(3) What is a product cipher?

(4) What is the difference between diffusion and confusion? How diffusion and confusion is achieved in Fiestels encryption algorithm?

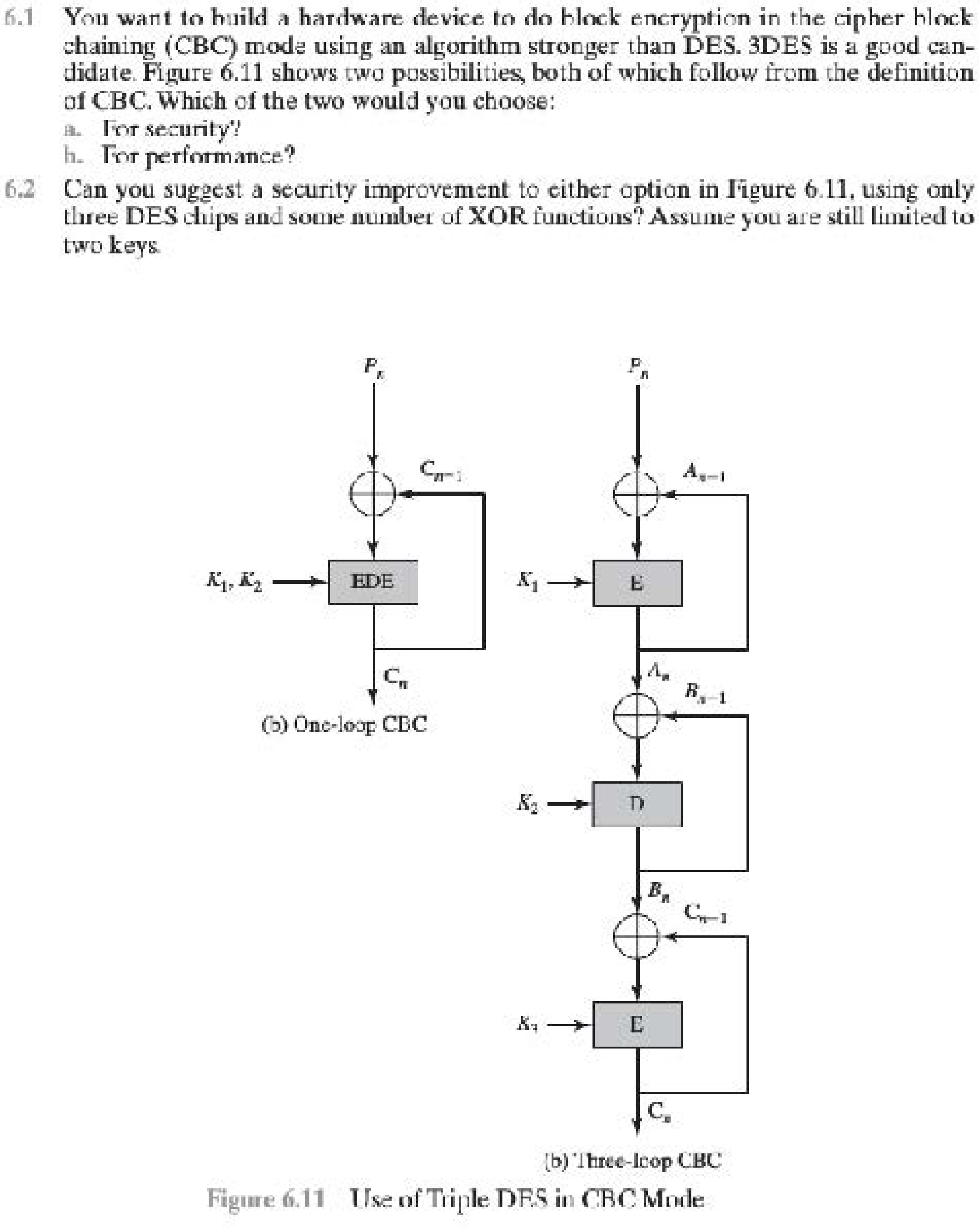
(5) What parameters and design choices determine the actual algorithm of a Feistel Cipher?

(6) The following are a list of questions for students to attempt at home to get a better grasp of the concepts discussed during the workshop.

  (a) Complete any questions that were not completed during the workshop.

  (b) What is avalanche effect? Why it is desired in encryption algorithms?

  (c) Write the block diagram for DES decryption algorithm.



6.1 You want to build a hardware device to do block encryption in the cipher block chaining (CBC) mode using an algorithm stronger than DES. 3DES is a good candidate. Figure 6.11 shows two possibilities, both of which follow from the definition of CBC. Which of the two would you choose:

a. For security?

b. For performance?

6.2 Can you suggest a security improvement to either option in Figure 6.11, using only three DES chips and some number of XOR functions? Assume you are still limited to two keys.

Figure 6.11 Use of Triple DES in CBC Mode

FIGURE 1. Q6.1 and 6.2