

King Fahd University of Petroleum and Minerals  
College of Computer Sciences and Engineering  
Department of Computer Engineering

COE 451 – Computer and Network Security (T151)

**Homework # 03 (due date & time: Sunday 04/10/2015 during class period)**

**Problem # 1:** Solve problem 4 of Chapter 3 of the textbook.

**Problem # 2:** Use the A5/1 algorithm. Suppose that, after a particular step, the values in the registers are

$$\begin{aligned} X = (x_0, x_1, \dots, x_{18}) &= (1010101010101010110) \\ Y = (y_0, y_1, \dots, y_{21}) &= (1100110001101100010011) \\ Z = (z_0, z_1, \dots, z_{22}) &= (11100101110000011000011) \end{aligned}$$

List the next 8 keystream bits and give the contents of  $X$ ,  $Y$ , and  $Z$  after the generation of each of these 8 bits.

**Problem # 3:** Consider a Feistel cipher with three rounds. Then the plaintext is denoted as  $P = (L_0, R_0)$  and the corresponding ciphertext is  $C = (L_3, R_3)$ . What is the **simplest form** of the ciphertext  $C$ , in terms of  $L_0$ ,  $R_0$ , and the subkey, for each of the following round functions?

- a.  $F(R_{i-1}, K_i) = K_i$
- b.  $F(R_{i-1}, K_i) = \overline{R_{i-1}}$ , where  $\overline{R_{i-1}}$  is the logical complement of  $R_{i-1}$
- c.  $F(R_{i-1}, K_i) = R_{i-1} \oplus K_i$

**Problem # 4:** Solve problem 13 of Chapter 3 of the textbook.

**Problem # 5:** Solve problem 25 of Chapter 3 of the textbook.

**Problem # 6:** Solve problem 43 of Chapter 3 of the textbook.