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

COE 451 – Computer and Network Security (T142)

<u>Homework # 03 *(due date & time: Thursday 05/03/2015 during class period)*</u>

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

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

$X = (x_0, x_1, \ldots, x_{18}) \quad = (\texttt{1010101000101010110})$
$Y = (y_0, y_1, \ldots, y_{21}) \quad = (\texttt{1100110001101100010001})$
$Z = (z_0, z_1, \ldots, z_{22}) \quad = (\texttt{11100101111000011000010})$

List the next 8 keystream bits and give the contents of *X*, *Y*, and *Z* after these 8 bits have been generated.

Problem # 3: Consider a Feistel cipher with four rounds. Then the plaintext is denoted as $P = (L_0, R_0)$ and the corresponding ciphertext is $C = (L_4, R_4)$. 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. $F(R_{i-1}, K_i) = 0$
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.