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

ICS 555 – Data Security and Encryption (T162)

Homework # 01 (due date & time: Wednesday 15/03/2017 during class period)

Problem # 1 – 20 points: Suppose that, after a particular step of A5/1, the values in the registers are

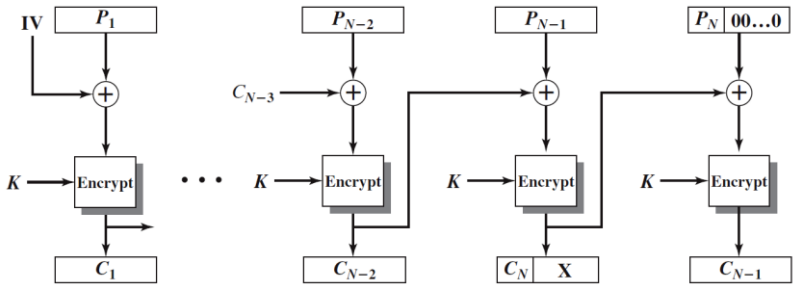
$X = (x_0, x_1, \ldots, x_{18})$ = (1010101010101010110)
$Y = (y_0, y_1, \ldots, y_{21})$ = (1100110001101100010011)
$Z = (z_0, z_1, \ldots, z_{22})$ = (1110010111000001100011)

a. **(5 points)** List the next 4 keystream bits.
b. **(15 points)** Give the contents of X, Y, and Z after the generation of each of these 4 bits.

Problem # 2 – 20 points; 10 points each: 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(s), for each of the following round functions?

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

Problem # 3 – 10 points: If needed, the ciphertext stealing (CTS) block cipher mode that is shown in the following figure uses padding with zeros for the last plaintext block. Describe how to decrypt C_{n-1} and C_n.



Problem # 4 – 25 points: Consider the RC4 stream cipher:

a. **(15 points)** Find the smallest upper bound on the size of the RC4 state space. That is, find an upper bound for the number of different states that are possible for the RC4 cipher. Hint: The RC4 cipher consists of a lookup table S, and two indices i and j. Count the number of possible distinct tables S and the number of distinct indices i and j, then compute the product of these numbers.
b. **(10 points)** Why is the size of the state space relevant when analyzing a stream cipher?

Problem # 5 – 25 points: Suppose that you know a MAC value X and the key K that was used to compute the MAC, but you do not know the original message.

a. **(15 points)** Show that you can construct a message M that also has its MAC equal to X. Note that we are assuming that you know the key K and the same key is used for both MAC computations.
b. **(10 points)** How much of the message M are you free to choose?