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

SEC 521 –Network Security (T151)

Homework # 01 (due date & time: Sunday 04/10/2015 during class period)

Problem # 1: Solve problem 2.2 of the 4th edition of William Stallings textbook.

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

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

List the next 4 keystream bits and give the contents of X, Y, and Z after the generation of each of these 4 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. $F(R_{i-1}, K_i) = \overline{R_{i-1}}$, 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 # 4: Solve problem 2.16 (**only part b**) of the 4th edition of William Stallings textbook.

Problem # 5: Use the "Repeated Squaring" method on p. 104 of the "Public-Key Cryptography" slides to compute 9^{25} *mod* 15. Show the power groupings and the steps.

Problem # 6: Solve problem 3.14 (**parts d and e**) of the 4th edition of William Stallings textbook.

Problem # 7: Solve problem 3.21 of the 4th edition of William Stallings textbook.

Problem # 8: Suppose that Bob uses the following variant of RSA. He first chooses N, then he finds two encryption exponents, e_0 and e_1, and the corresponding decryption exponents d_0 and d_1. He asks Alice to encrypt her message M to him by first computing $C_0 = M^{e0}$ mod N, then encrypting C_0 to obtain the ciphertext, $C_1 = C_0^{e1}$ mod N. Alice then sends C_1 to Bob. Does this double encryption increase the security as compared to a single RSA encryption? Why or why not?