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

COE 451 – Computer and Network Security (T142)

Homework # 04 ***(due date & time: Thursday 12/03/2015 during class period)***

Problem # 1: Suppose that Alice's RSA public key is $(N, e) = (33, 7)$

a. Find her private key, d.
b. If Bob encrypts the message $M = 17$ using Alice's public key, what is the ciphertext C? Show that Alice can decrypt C to obtain M.
c. Let S be the result when Alice digitally signs the message $M = 19$. What is S? If Bob receives M and S, explain the process Bob will use to verify the signature and show that in this particular case, the signature verification succeeds.

Problem # 2: Solve problem 10 (only parts **b** and **d**, and use a 128-bit symmetric key for part **d**) of Chapter 4 of the textbook.

Problem # 3: Suppose that Bob's knapsack private key consists of (3, 5, 10, 21) along with the multiplier $m^{-1} = 6$ and modulus $n = 41$.

a. Find the plaintext given the ciphertext $C = 18$. Give your answer in binary.
b. Find m and the public key.

Problem # 4: Consider the knapsack cryptosystem. Suppose the public key consists of (15, 25, 1, 27) and $n = 44$.

a. Find the private key, assuming $m = 5$.
b. Encrypt the message $M = 1011$ (given in binary). Give your result in decimal.

Problem # 5: Solve problem 30 of Chapter 4 of the textbook.

Problem # 6: Use the repeated squaring technique to compute 7^{27} *mod* 11. Show the power groupings and the steps.