

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 # 04 (due date & time: Tuesday 13/10/2015 during class period)

Problem # 1: Suppose that Alice's RSA public key is $(N, e) = (33, 13)$

- Find her private key, d .
- If Bob encrypts the message $M = 19$ using Alice's public key, what is the ciphertext C ? Show that Alice can decrypt C to obtain M .
- Let S be the result when Alice digitally signs the message $M = 17$. 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 256-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 $n = 47$.

- Find the plaintext given the ciphertext $C = 26$. Give your answer in binary.
- Find m and the public key.

Problem # 4: Consider the knapsack cryptosystem. Suppose the public key consists of $(21, 35, 33, 36)$ and $n = 44$.

- Find the private key, assuming $m = 7$.
- Encrypt the message $M = 1001$ (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 $9^{25} \text{ mod } 15$. Show the power groupings and the steps.