**Description for: CS 492 Homework 3**

Public Key Cryptography

Complete the problems below and submit this word document with the solution to the questions here.

Name:  
 Matthew Krieger

Problem 1 (book 4.21):

Suppose that for the knapsack cryptosystem, the superincreasing knapsack is (3,5,12,23) with n=47 and m=6

1. What are the public and private keys?

3 x 6 mod (47) = 18

5 x 6 mod (47) = 30

12 x 6 mod (47) = 25

23 x 6 mod (47) = 44

**Public Key: {18, 30, 25, 44}**

**Private Key: {3, 5, 12, 23}**

1. Encrypt the message M = 1101 given in binary. Give your result in decimal

**(1 x 18) + (1 x 30) + (0 x 25) + (1 x 44) = 92**

**92**

Problem 2 (book 4.6):

Suppose that Alice’s RSA public key is (N,e) = (33,3) and her private key is d=7.

1. If Bob encrypts the message M = 19 using Alice’s public key
   1. what is the ciphertext C?

C = Me mod N

(*N,e*) = (33,3)

C = 193 mod 33

193 = 6859

C = 6859 mod 33 = 28

**C = 28, ciphertext sent to Alice**

* 1. Show that Alice can decrypt C to obtain M

M = Cd mod N

M = 287 mod 33

(n,d) = (33, 7)

287 = 13492928512

M = 13492928512 mod 33 = 19

**M = 19, the original message from Bob**

1. Let S be the result when Alice digitally signs the message M = 25.
   1. What is S?

S = Md mod N

S = 257 mod N

S = 6103515625 mod 33

**S = 31**

* 1. If Bob receives M and S, show how Bob verifies the signature

M = 25, S = 31

Se mod N = M

313 mod 33

29791 mod 33 = 25

**25 = M**

Problem 3

Alice and Bob are making their wills. For the final will they want to send a copy to their attorney Charlie that only Charlie can read and that shows both Alice and Bob have approved it. Using the notation in the slides (same as that in the book). What would be the notation of a message that accomplishes this task?

Assumption: Alice & Bob each have their own wills:

{[M1]Alice , [M2]Bob}Charlie