Problem 1

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

What are the public and private keys?

$$\begin{aligned} mm^{-1} &\equiv 1 \pmod{n} \\ 6m^{-1} &\equiv 1 \pmod{47} \end{aligned}$$

$$\begin{aligned} 47 &= 6(7) + 5 \\ 6 &= 5(1) + 1 \end{aligned}$$

$$\begin{aligned} 5 &= 47 - 6(7) \\ 1 &= 6 - 5(1) \end{aligned}$$

$$\begin{aligned} 1 &= 6 - (47 - 6(7))(1) \\ 1 &= 6 - (47 - 6(7)) \\ 1 &= 47(1) - 6(6) \end{aligned}$$

Private key: 6
Public key: $(18, 30, 25, 44)$

Encrypt the message $M = 1101$

$$C = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 18 \\ 30 \\ 25 \\ 44 \end{bmatrix} = 92$$

Problem 2

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

If Bob encrypts the message $M = 19$, what is the ciphertext?

$$\begin{aligned} C &\equiv M^e \pmod{n} \\ 28 &\equiv 19^3 \pmod{33} \end{aligned}$$

Show that Alice can decrypt C to obtain M

$$\begin{aligned} (m^e)^d &\equiv m \pmod{n} \\ C^d &\equiv m \pmod{n} \\ 28^7 &\equiv 19 \pmod{33} \end{aligned}$$

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

$$\begin{aligned} S &\equiv M^d \pmod{n} \\ 31 &\equiv 25^7 \pmod{33} \end{aligned}$$

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

$$\begin{aligned} M' &\equiv S^e \pmod{n} \\ 25 &\equiv 31^3 \pmod{33} \\ M &= M' \end{aligned}$$

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?

$$\{[[M]_a]_b\}_c$$