Homework 3

Antonio Zea Jr

October 3, 2022

Abstract

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.
Be sure to show your work related to each problem to receive full credit for your answer.

Problem 1 (similar, but not identical to book problem 4.21):

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?

Private: SIK $(3, 5, 12, 23)$ $n = 47$ and $m = 6$

$3 \cdot 6 \mod 47 = 18$
$5 \cdot 6 \mod 47 = 30$
$12 \cdot 6 \mod 47 = 25$
$23 \cdot 6 \mod 47 = 44$

Public: GK $(18, 30, 25, 44)$

Encrypt the message $M = 1011$ given in binary. Give your result in decimal

$6^{-1} \mod 47$

$$\begin{aligned} 47 &= 6(7) + 5 & 5 &= 47 - 6(7) \\ 6 &= 5(1) + 1 & 1 &= 6 - 5(1) \end{aligned} \qquad \begin{aligned} 1 =& 6 - 5(1) \\ 1 =& 6 - (47 - 6(7)) \\ 1 =& 6(8) - 47 \end{aligned} \qquad \therefore 6^{-1} \mod 47 = 8$$

$M = 1011_2 \implies 11_{10}$
$1 \cdot 18 + 0 \cdot 30 + 1 \cdot 25 + 1 \cdot 44 = 87$

Problem 2 (similar, but not identical to book problem book 4.6):

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

If Bob encrypts the message $M = 17$ using Alice's public key

What is the ciphertext C?

Public Key: $(N, e) = (33, 3)$
Private Key $d = 7$

$$M = 17$$
$$\begin{aligned} C =& M^e \mod N \\ =& 17^3 \mod 33 = 29 \end{aligned}$$

Show that Alice can decrypt C to obtain M

$$\begin{aligned} M =& C^d \mod N \\ =& 29^7 \mod 33 = 17 \end{aligned}$$

Let S be the result when Alice digitally signs the message $M = 23$.

What is S?

$M = 23$ and $d = 7$

$$S = 23^7 \mod 33 = 23$$

If Bob recieves M and S show how Bob verifies the signature

$S = 23$ and $(N, e) = (33, 3)$

$$M = 23^3 \mod 33 = 23$$

$\therefore$ Alice digitially signed this message

Problem 3

Alice and Bob are making a joint will (i.e. M represents the single will for both of them). For the final will they want to send a copy to their attorney Charlie that only Charlie can read and that shows that 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?

$\{[[M]_{\text{Bob}}]_{\text{Alice}}\}_{\text{Charlie}}$