CS430 Project 3

1. 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, what is the ciphertext C? Show that Alice can decrypt C to obtain M.

Encrypt

C = M^e mod N

C = 19^3 mod 33

C = 28

Decrypt

M = C^d mod(N)

M = 28^7 mod(33)

M = 19

* 1. Let S be the result when Alice digitally signs the message M = 25. 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.

S = M^d mod N

S = 25^7 mod 33

S = 31

Verify

M = S^e mod N

M = 31^3 mod 33

25 = 25

1. Consider the knapsack cryptosystem. Suppose the public key consists of (18, 30, 7, 26) and n = 47.
   1. Find the private key, assuming m = 6.

X\*6 mod 47 = 26

6x = 26(mod47) a = 47 b = 6

47 = 6 \* 7 + 5 5 = 47-6\*7 5 = a-7b

6 = 5 \* 1 + 1 1 = 6-5\*1 1 = b – (a-7b)

1 = 8b-a

8\*6x = 26\*8(mod 47)

48x = 208(mod 47)

X= 20(mod 47)

X = 20

X\*6 mod 47 = 7

6x = 7(mod47) a = 47 b = 6

47 = 6 \* 7 + 5 5 = 47-6\*7 5 = a-7b

6 = 5 \* 1 + 1 1 = 6-5\*1 1 = b – (a-7b)

1 = 8b-a

8\*6x = 7\*8(mod 47)

48x = 56(mod 47)

X= 9(mod 47)

X = 9

X\*6 mod 47 = 30

6x = 30(mod47) a = 47 b = 6

47 = 6 \* 7 + 5 5 = 47-6\*7 5 = a-7b

6 = 5 \* 1 + 1 1 = 6-5\*1 1 = b – (a-7b)

1 = 8b-a

8\*6x = 30\*8(mod 47)

48x = 240(mod 47)

X= 5(mod 47)

X = 5

X\*6 mod 47 = 18

6x = 18 (mod47) a = 47 b = 6

47 = 6 \* 7 + 5 5 = 47-6\*7 5 = a-7b

6 = 5 \* 1 + 1 1 = 6-5\*1 1 = b – (a-7b)

1 = 8b-a

8\*6x = 18\*8(mod 47)

48x = 144(mod 47)

X= 3(mod 47)

X = 3

SIK = {3, 5, 9, 20}

m-1 mod n = 6-1 mod 47

Private Key = {3, 5, 9, 20} and 6-1 mod 47 = 8

Thus M = 1100 because 3+5=8

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

Assuming we are using the SIK from before ({3, 5, 9, 20}) and n = 47

Relatively prime m = 12 because 12-1 mod 47 = 4

Then to get to the general knapsack we take the SIK and do some modular multiplication.

Thus:

3m = 3 \* 12 = 36 mod 47

5m = 5 \* 12 = 13 mod 47

9m = 9 \* 12 = 14 mod 47

20m = 20 \* 12 = 5 mod 47

The resulting general knapsack is {36,13,14,5}

Then the encrypted message is 36+13+5=54

Thus is ciphertext decimal is 54