HW03- Nicolas Dalton

Problem #1:

Part 1:

Compute N:

p = 11

q = 7

p * q

11*7 = 77

N = 77

(p-1) * (q-1) = r

(11-1) * (7-1) = r

(10) * (6) = 60

Generate e:

Greatest Common Divisor of 7 and 60 = 1

e = 7

Find d:

e * d mod (p-1)*(q-1) = 1

e * d mod 60 = 1

7 * d mod 60 = 1

7 * 43 mod 60 = 1

d = 43

Part #2:

Alice's public key = (N,e) -> (21,5)

name = "NICOLAS DALTON"

ASCII name = 78 73 67 79 76 65 83 32 68 65 76 84 79 78

Encrypt name = M^e mod N

7^5 mod 21 = 7

8^5 mod 21 = 8

7^5 mod 21 = 7

3^5 mod 21 = 12

6^5 mod 21 = 6

7^5 mod 21 = 7

7^5 mod 21 = 7

9^5 mod 21 = 18

7^5 mod 21 = 7

6^5 mod 21 = 6

6^5 mod 21 = 6

5^5 mod 21 = 17

8^5 mod 21 = 8

3^5 mod 21 = 12

3^5 mod 21 = 12

2^5 mod 21 = 11

6^5 mod 21 = 6

5^5 mod 21 = 17

7^5 mod 21 = 7

6^5 mod 21 = 6

8^5 mod 21 = 8

4^5 mod 21 = 16

7^5 mod 21 = 7

9^5 mod 21 = 18

7^5 mod 21 = 7

8^5 mod 21 = 8

Encryption that only Alice can decrypt is:

07 08 07 12 06 07 07 18 07 06 06 17 08 12 12 11 06 17 07 06 08 16 07 18 07 08

Alice can use her private key to decrypt this

Part #3:

Signature name "NICOLAS DALTON"

private key = (N,d) = (77,43)

ASCII name = 78 73 67 79 76 65 83 32 68 65 76 84 79 78

Private key = character^d mod N

7^{43} mod 77 = 35	8^{43} mod 77 = 50
7^{43} mod 77 = 35	3^{43} mod 77 = 38
6^{43} mod 77 = 62	7^{43} mod 77 = 35
7^{43} mod 77 = 35	9^{43} mod 77 = 58
7^{43} mod 77 = 35	6^{43} mod 77 = 62
6^{43} mod 77 = 62	5^{43} mod 77 = 26
8^{43} mod 77 = 50	3^{43} mod 77 = 38

$3^{43} \bmod 77 = 38$	$2^{43} \bmod 77 = 30$
$6^{43} \bmod 77 = 62$	$8^{43} \bmod 77 = 50$
$6^{43} \bmod 77 = 62$	$5^{43} \bmod 77 = 26$
$7^{43} \bmod 77 = 35$	$6^{43} \bmod 77 = 62$
$8^{43} \bmod 77 = 50$	$4^{43} \bmod 77 = 53$
$7^{43} \bmod 77 = 35$	$9^{43} \bmod 77 = 58$
$7^{43} \bmod 77 = 35$	$8^{43} \bmod 77 = 50$

signature =
35 50 35 38 62 35 35 58 35 62 62 26 50 38 38 30 62 50 62 26 35 62 50 53 35 58 35 50
Alice can verify this signature by using my public key

Part #4:
message = "NICOLAS DALTON"

Message encrypted with Alice's public key from part #2:
07 08 07 12 06 07 07 18 07 06 06 17 08 12 12 11 06 17 07 06 08 16 07 18 07 08
And then signing it with my private key:

$7^{43} \bmod 77 = 35$	$8^{43} \bmod 77 = 50$	$7^{43} \bmod 77 = 35$	$1^{43} \bmod 77 = 01$
$2^{43} \bmod 77 = 30$	$6^{43} \bmod 77 = 62$	$7^{43} \bmod 77 = 35$	$7^{43} \bmod 77 = 35$
$1^{43} \bmod 77 = 01$	$8^{43} \bmod 77 = 50$	$7^{43} \bmod 77 = 35$	$6^{43} \bmod 77 = 62$
$6^{43} \bmod 77 = 62$	$1^{43} \bmod 77 = 01$	$7^{43} \bmod 77 = 35$	$8^{43} \bmod 77 = 50$
$1^{43} \bmod 77 = 01$	$2^{43} \bmod 77 = 30$	$1^{43} \bmod 77 = 01$	$2^{43} \bmod 77 = 30$
$1^{43} \bmod 77 = 01$	$1^{43} \bmod 77 = 01$	$6^{43} \bmod 77 = 62$	$1^{43} \bmod 77 = 01$
$7^{43} \bmod 77 = 35$	$6^{43} \bmod 77 = 62$	$8^{43} \bmod 77 = 50$	$1^{43} \bmod 77 = 01$
$6^{43} \bmod 77 = 62$	$7^{43} \bmod 77 = 35$	$1^{43} \bmod 77 = 01$	$8^{43} \bmod 77 = 50$
$7^{43} \bmod 77 = 35$	$8^{43} \bmod 77 = 50$		

Encrypted and then signed the message:
35 50 35 01 30 62 35 35 01 50 35 62 62 01 35 50 01 30 01 30 01 01 62 01 35 62
50 01 62 35 01 50 35 50
Alice first can verify that I am the sender and then decrypt the message

Part #5:
My digital signature from part #3:
35 50 35 38 62 35 35 58 35 62 62 26 50 38 38 30 62 50 62 26 35 62 50 53 35 58 35 50

$3^{5} \bmod 21 = 12$	$5^{5} \bmod 21 = 17$

$5^5 \bmod 21 = 17$

$3^5 \bmod 21 = 12$

$3^5 \bmod 21 = 12$

$6^5 \bmod 21 = 6$

$3^5 \bmod 21 = 12$

$5^5 \bmod 21 = 17$

$3^5 \bmod 21 = 12$

$6^5 \bmod 21 = 6$

$6^5 \bmod 21 = 6$

$2^5 \bmod 21 = 11$

$5^5 \bmod 21 = 17$

$3^5 \bmod 21 = 12$

$3^5 \bmod 21 = 12$

$3^5 \bmod 21 = 12$

$6^5 \bmod 21 = 6$

$2^5 \bmod 21 = 11$

$3^5 \bmod 21 = 12$

$6^5 \bmod 21 = 6$

$5^5 \bmod 21 = 17$

$5^5 \bmod 21 = 17$

$3^5 \bmod 21 = 12$

$5^5 \bmod 21 = 17$

$3^5 \bmod 21 = 12$

$5^5 \bmod 21 = 17$

$0^5 \bmod 21 = 0$

$5^5 \bmod 21 = 17$

$8^5 \bmod 21 = 8$

$2^5 \bmod 21 = 11$

$5^5 \bmod 21 = 17$

$8^5 \bmod 21 = 8$

$5^5 \bmod 21 = 17$

$2^5 \bmod 21 = 11$

$2^5 \bmod 21 = 11$

$6^5 \bmod 21 = 6$

$0^5 \bmod 21 = 0$

$8^5 \bmod 21 = 8$

$8^5 \bmod 21 = 8$

$0^5 \bmod 21 = 0$

$2^5 \bmod 21 = 11$

$6^5 \bmod 21 = 6$

$5^5 \bmod 21 = 17$

$2^5 \bmod 21 = 11$

$0^5 \bmod 21 = 0$

$3^5 \bmod 21 = 12$

$5^5 \bmod 21 = 17$

$8^5 \bmod 21 = 8$

$5^5 \bmod 21 = 17$

$0^5 \bmod 21 = 0$

Signed, then encrypted message:
12 17 17 00 12 17 12 08 06 11 12 17 12 08 06 11 06 11 11 06 17 00
12 08 12 08 12 00 06 11 11 06 12 17 06 11 17 00 17 12 12 17 17 08
12 17 17 00

Alice can first decrypt the message and then verify I am the sender.

Alice can verify it is me by using my public key, and then she can decrypt the message with her private key

Problem #2:

Alice's private value, a = 11

Bob's private value, b = 13

g = 10 p = 541

Alice sends to Bob:

$g^a \bmod p$

$10^{11} \bmod 541 = 297$

Bob sends to Alice:

$g^b \bmod p$

$10^{13} \bmod 541 = 486$

Now that both Alice and Bob have sent their keys

Alice can compute the symmetric key:

$(g^b \bmod p)^a$

$(486)^{11} \bmod 541 = 511$

Bob can compute symmetric key:

$(g^a \bmod p)^b$

$(297)^{13} \bmod 541 = 511$

511 is the symmetric key for Alice and Bob.