1]

p=13 & q=3

n = p\*q = 13\*3 = 39

Q(n) = (p-1)\*(q-1) = 12\*2 = 24

We choose e = 7 such that (GCD (e, Q(n)) = 1)

Now we find d such that

ed = 1 mod Q(n)

There fore d = 7.

Thus private key = (7,39)

Public key = (7,39)

The last two digits of my N number are 0 & 2 (N13522702)

Message

m = 02 mod 38 = 2

Encrypting the message

c = (m^e) mod n

= (2^7) mod 39

= 128 mod 39

= 11

Encrypted message is 11

Decrypting the message

m = (c^d) mod n

= (11^7) mod 39

= 2

Original message is 2

2]

We take

n = 23

g = 5

Alice secret key = 10 (a)

Bobs secret key = 12 (b)

Alice’s public key

A = (g^a) mod n

= (5^10) mod 23

= ((5^4)\*(5^4)\*(5^2)) mod 23

Since

5^2 mod 23 = 2

There fore

5^4 mod 23 = 4

A = (4\*4\*2) mod 23

= 32 mod 23

= 9

Bobs public key

B = (g^b) mod n

= (5^12) mod 23

= ((5^4)\*(5^4)\*(5^4)) mod 23

= (4\*4\*4) mod 23

= 64 mod 23

= 18

Secret key calculated by Alice

Ka = (B^a) mod n

= (18^10) mod 23

= ((18^4)\*(18^4)\*(18^2)) mod 23

Since

18^2 mod 23 = 2

There fore

18^4 mod 23 = 4

Ka =(4\*4\*2) mod 23

= 9

Secret Key calculated by Bob

Kb = (A^b) mod n

= (9^12) mod 23

= ((9^4)\*(9^4)\*(9^4)) mod 23

Since

9^2 mod 23 = 12

There fore

9^4 mod 23 = 144 mod 23 = 6

Kb = (6\*6\*6) mod 23

= 9

there fore

Ka = Kb