DALHOUSIE UNIVERSITY

Network Security (CSCI-6708)

Assignment - 7

Shivam Gupta
B00810723

Question 1.

a) p= 7
q= 11
M= 6

Finding e:
n=pq
n= 11x7= 77

p-1= 6
q-1= 10
p-1 x q-1= 60

here 1,2,3,4,5,6 are factors of 60.

e= 7

Finding d:
ed mod (p-1)(q-1) = 1

7d mod 60 = 1
7d = 61 NO
7d= 121 NO
7d= 181 NO
7d= 241 NO
7d= 301 YES
d= 43

Public Key K1= (7,77)
Private key K2= (43, 77)

Encrypted message:
C= M^e mod n
C= 6^7 mod 77
C= (6^2 . 6^2 . 6^2. 6) mod 77
C= (36.36.36.6) mod 77
C= (1296. 216) mod 77
C= (64. 62) mod 77
C= 3968 mod 77
C= 41

b) p=11
q=13
M=9

n= 11x13= 143
n=143

p-1 x q-1 = 10x12 = 120
(p-1).(q-1) = 120

here 1,2,3,4,5,6 are factors of 120.

e= 7

ed mod (p-1)(q-1)=1
7d mod 120=1
7d=121 NO
7d= 241 NO
7d= 361 NO
7d= 481 NO
7d= 601 NO
7d= 721 YES

d=103

Public key = (7,143)
Private key= (103,143)

Encrypted message:
C= M^e mod n
C= 9^7 mod 143
C= 9^2. 9^2. 9^2.9 mod 143
C= 81.81.81.9 mod 143
C= 6561. 729 mod 143
C= 126. 14 mod 143
C= 1764 mod 143
C= 48

c) p=17
q=31
M=5
n=17x31= 527

(p-1).(q-1)= 16 x 30= 480

Here 1,2,3,4,5,6 are factor of 480
e=7

ed mod (p-1)(q-1)=1
7d mod 480=1
7d=481 NO
7d= 961 NO
7d= 1441 NO
7d= 1921 NO
7d= 2401 YES

d= 343

public key= (7,527)
private key = (343,527)

Encrypted message:
C= M^e mod n
C= 5^7 mod 527
C= 5^2. 5^2. 5^2.5 mod 527
C= 25.25.25.5 mod 527
C= 625. 125 mod 527
C= 98.125 mod 527
C= 12250 mod 527
C= 129

Question 2: C=10

Public key: (5,35)

n=pq

35=pq

e=5

Let’s get the factors of 35: 7x5, 35x1.

Case 1:

P=7

Q=5 or Vice Versa p=5 and q=7

p-1 x q-1 = 6 x 4 = 24

1,2,3,4, are factors of 24.

e=5 which is already given (matched)

ed mod (p-1)(q-1)=1

5d mod 24=1

5d=25 yes

d=5

M= C^d mod n

M= 10^5 mod 35

M= 100.100.10 mod 35

M= 30.30.10 mod 35

M= 900.10 mod 35

M= 25.10 mod 35

M= 5

Case 2:

p=35

q=1

n=35

p-1 x q-1 = 34 x 0= 0

we can’t get factors of 0, so this case is invalid.

Out of 2 cases, case 2 is invalid, so Case 1 is correct, which means:

M= 5, the plain text message is 5.

Yes, we can determine the plaintext message M by trail and error or brute force method as I did above.