Q1.

Given, P=3, Q=11, e=7, plaintext=5

Find d, ciphertext

Ans:

N= P*Q = 3*11 = 33

Z= (P-1) * (Q-1) = 2*10 = 20

Now,

d can be any prime number that have only one common factor with Z, i.e 1

Here, we can choose 3 or 7

also, From the below Formula we can find d.

e*d = 20*n+1

so,

For n=1, 7*d = 21 ➔ so, **d=3**

Next step to Find Ciphertext

C = E(M)
  = M^e mod N
  = (5^7)mod 33
  = 14

So, d= 3 and Ciphertext = 14

Q2.

Bob	Eve	Alice
↓		↑
msg		MD
↓		↑
MD		hash
↓		↑
{(Msg)} + kab		msg' + SA'
↓		↑
SA		
↓ +kab		
{msg + SA} K_{AB} →	→	kA_B{ngg + sa}