a) **Using MIT public key encryption with numeric value of each alphabet is its lexical position (eg a=1,b=2, etc), encrypt the text "computernetwork". Take p=5, q=11 and d=27. Also compute e.**

Solution:

In this scenario we shall go RSA which is Asymmetric (Public Key Private Key) Key algorithm

As given
P=5
Q=11

N=P*Q=5*11=55
D=27

E= 3 ((5-1)(11-1) = 40 → 2,5)

ABCDE FGHIJ KLMNO PQRST UVWXY Z

PT=Plain Text

PT→	**C**	**O**	**M**	**P**	**U**	**T**	**E**	**R**	**N**	**E**	**T**	**W**	**O**	**R**	**K**	**S**
No. for PT→	3	15	13	16	21	20	5	18	14	5	20	23	15	18	11	19
CT→	27															

PT=C=3

$CT=PT^E \bmod N$

$CT = 3^3 \text{ MOD } 55 = 27$
$CT = 15^3 \text{ MOD } 55 =$
$CT = 13^3 \text{ MOD } 55 =$
$CT = 16^7 \text{ MOD } 55 =$
$CT = 15^7 \text{ MOD } 55 =$
$CT = 15^7 \text{ MOD } 55 =$
$CT = 15^7 \text{ MOD } 55 =$

PT= 15 (27) mod 55

Illustration for 3^3 MOD 55

→ $3^1 \bmod 55 = 3 \bmod 55 = 3$
→ $3^2 \bmod 55 = 9 \bmod 55 = 9$
→ $3^4 \bmod 55 = (3^2)^2 = 9^2 = 81 \bmod 55 = 25$
→ $3^8 \bmod 55 = (3^4)^*(3^4) = 20$
→ $3^9 \bmod 55 = (3^8)^*(3^1) = 20*3 = 5$

PT= 5 (27) mod 55

27 (1) mod 55 = 27
27 (2) mod 55 = 14
27 (4) mod 55 = 31
27 (8) mod 55 = 26
27 (16) mod 55 = 16
(27 (16) * 27 (8) * 27 (2) * 27 (1)) mod 55 = 16*26*14*27 = 157248-157245= 3