```
RSA Solved Examples
1
                              n= 143
    P, 9 = 13,11
                              P(n)=120
                 13, 9cd (13, 120)=1
     d= lepens xi)+1
        = 120+1 - 9.30 (i=1)
         \frac{-(120\times2)+1}{13} = \frac{241}{13} = 98.53
         = (360+1) = 361 = 27,76
          = (20 \times 4) + 1 = 481 - 37,
= 13
     d=37)
   cipnertext = c = Me mod n
    M = 13
                  m < n
          = 13 mod 143
(13 mod 143) × (134 mod 143) ×
                 (138 mod 143) mod 193
       = (13×26×104×91) mod 143
   C - 52
```

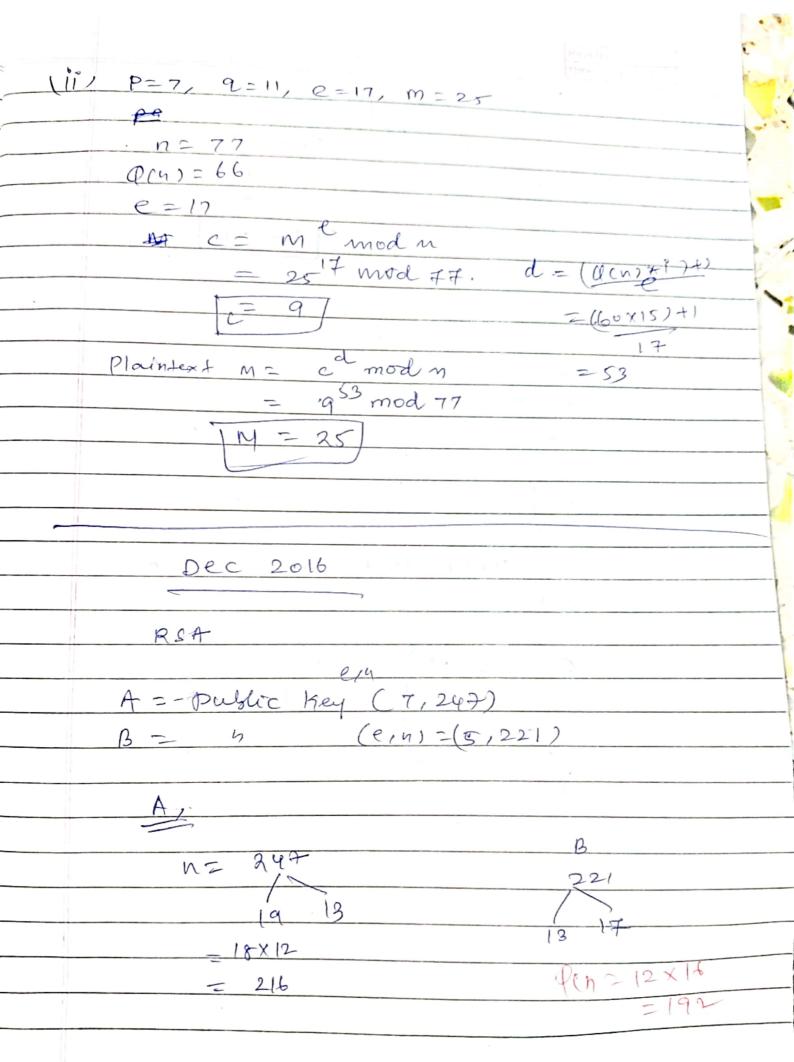
MP= col mod n = (52) mod n. = (52)32 x (52) x 52 ) mod 143 = (130 x 26 x 52) mod 143 Prime numbers 3, #1) C=3 m = 59, - Calculate Private keyd and Cipher text c. => P/9 = 3,711 n=21Q(n) = 20, e-3 given d= (20 X1)+1 = 21 = 7. 0 = 7 C = Me mod n = (59)3 mod 33 mod 3 = (592 mod 33) x (59 mod 33) (16 x 26) mod 33

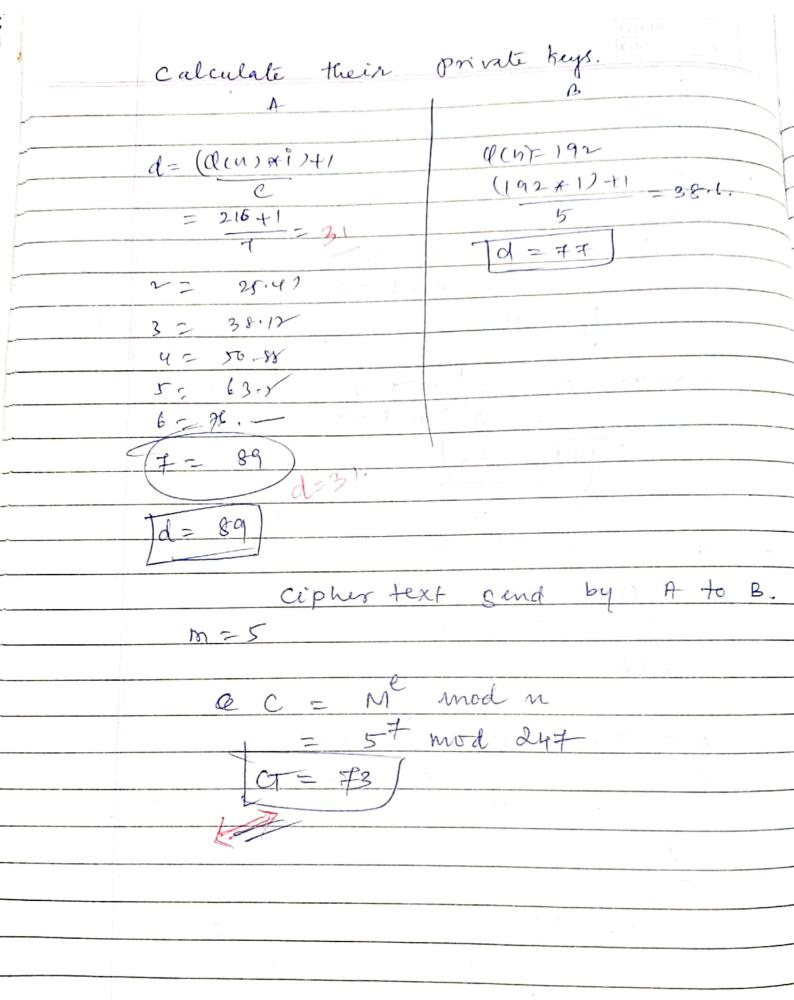
A WIND WIND WIND WINDS  $M = c^{d} \mod n$   $= 20^{7} \mod 33$ = 1204 mod 33 x 202 mod 33 x 20 mod 337 mod 33 = (41 × 4×4] mod 33 /(1280 mod 33) 3) Prime numbers 7,17 PT = 10 " (E) (Cn) = 96. gcd (5,96)=1 we select e=5,  $d = \frac{(96 \times 1) + 1}{6} = \frac{19.4}{6}$ =  $(96 \times 2_{+1}) = 38.6.$  $=(96 \times 3)+1=57-8$ d = (96 x4)+1 = 77. d= 77 = M mod n = 10<sup>5</sup> mod 11<sup>9</sup> = (10<sup>4</sup> ×10) mod 11<sup>9</sup> = 40

M= cd modn = 40<sup>77</sup> mod 119 = 40<sup>37</sup> x 40<sup>3</sup> x 40<sup>8</sup> x 40<sup>8</sup> x 40<sup>8</sup> x 10<sup>1</sup> 4776 14 24 = 10 72 X P19 = 13,17 M = 12e=19. 1= 221 acn)=192 e=19. d = (Q(a)\*i)+1  $= \frac{(192 \times 1) + 1}{89} = \frac{193}{19} = 10.1$ 

Public Key: Se, n3 = 519, 2213 Private Key { d, n3 = \$91, 2213 C= Me mod n - 1219 mod 221 M= cd mod n = 18191 mod 221 enouption by (t)=17. find corresponding private truy d 11 = P × 9 (Q(n) x1)+1 = (160x1)+1 = 9. 160 ×12) +1 = 113,

MU.15 Using RSA algo
(i) P=3, 9=11, e=7, m=12 (i) P=7, 9=11, e=17, m=25 (ii) find the Corresponding d's fur (i) and (ii) and ecrypt the cipher text,
$(i) P_1 Q = 3, 11$ $n = 33$
Q(n)= 20
C= Me mod u
$= 12^{7} \mod 33$
C = 12
d= (Q(n) *i) +1
C
d=(20x1)+1
7
d=3
M= cd mod n
$= 12^3 \mod n$
= 12 <sup>3</sup> mod 33
[P] = [2]





De c' 15 RSAI (e,n) = (7,119) Calculate c(cu)= ? Céphertext =? M=10% l(cn)= 160/1. T 17 ciphertext 6 X16 C = Me mod n = 10 + mod 119