Part - B :-

1). perform encryption and decryption for RSA algorithm :-

p = 3, q = 11, e = 7, d = ? M = 5

Key Generation :

$n = p \times q$

$= 3 \times 11$

$= 33.$

$\phi(n) = n - 1$

$\phi(pq) = (p-1)(q-1).$

$= (3-1)(11-1)$

$= 20$

$Gcd((\phi(n), e) = 1$

$Gcd(20, 7) = 1$

$e = 7$

$d = e^{-1} \bmod n$

$= 7^{-1} \bmod 20$

$d \equiv e^{-1} \bmod \phi(n)$

$20 \times 1 = \frac{20+1}{7} = \frac{21}{7} = 3$

$\boxed{d = 3}$

$PU = \{e, n\} = \{7, 33\}$

$PR = \{d, n\} = \{3, 33\}$

Encryption:

$C = m^e \bmod n$

$= 5^7 \bmod 33$

$5 \bmod 33 = 5$

$5^2 \bmod 33 = 25$

$5^4 \bmod 33 = (5^2 \times 5^2) \bmod 33$

$= (25 \times 25) \bmod 33$

$= 625 \bmod 33$

$= 31.$

$5^7 \bmod 33 = (5^4 \times 5^2 \times 5) \bmod 33$

$= 31 \times 25 \times 5 \bmod 33$

$= 3875 \bmod 33$

$C = 14$

Decryption:-

$M = C^d \bmod n$

$= 14^3 \bmod 33$

$14 \bmod 33 = 14$

$14^2 \bmod 33 = (14 \times 14) \bmod 33$

$= 196 \bmod 33$

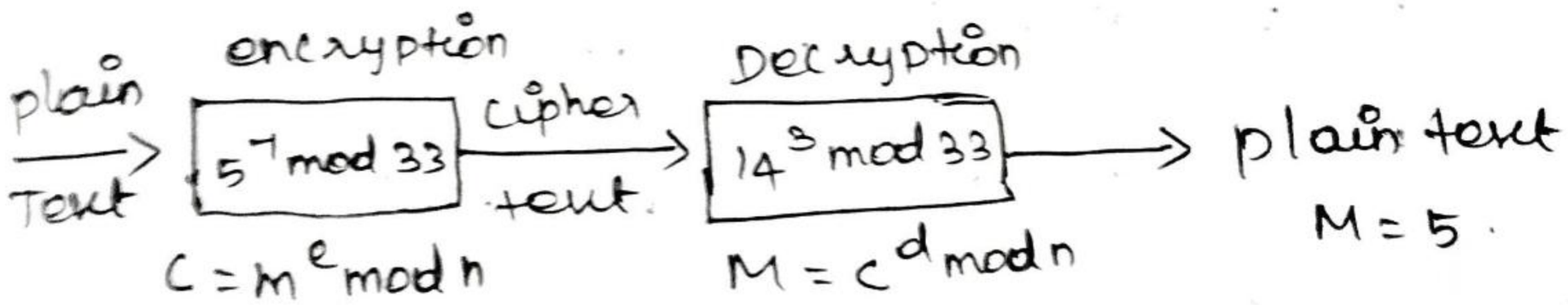
$= 31$ . . .)

$14^3 \bmod 33 = (14^2 \times 14) \bmod 33$

$= 31 \times 14 \bmod 33$

$= 434 \bmod 33$

$M = 5$



3) perform encryption and decryption for the system.

$p = 7$, $q = 11$, $e = 17$, $M = 8$.

$n = p \times q$

$= 7 \times 11$.

$n = 77$

$\phi(pq) = (p-1)(q-1)$

$= (7-1)(11-1)$

$= 6 \times 10$

$\phi(pq) = 60$

$GCD(\phi(n), e) = 1$

$GCD(60, e) = 1$

$e = 17$

$d = e^{-1} \bmod \phi(n)$

$= 17^{-1} \bmod 60$

$60 \times 1 = \frac{60+1}{17} \neq 0$

$60 \times 2 = \frac{120+1}{17} \neq 0$

$\vdots$

$60 \times 5 = \frac{901}{17} = 53$

$\boxed{d = 53}$

$PU = \{e, n\} = \{17, 77\}$

$PR = \{d, n\} = \{53, 77\}$

Encryption:-

$C = M^e \bmod n$

$= 8^{17} \bmod 77$

$8 \bmod 77 \Rightarrow 8$

$8^2 \bmod 77 = 64$

$8^4 \bmod 77 = (8^2 \times 8^2) \bmod 77$

$= 64 \times 64 \bmod 77$

$= 4096 \bmod 77$

$= 15$

$8^8 \bmod 77 = (8^4 \times 8^4) \bmod 77$

$= 15 \times 15 \bmod 77$

$= 225 \bmod 77$

$= 71.$

$8^{17} \bmod 77 = (8^8 \times 8^8 \times 8) \bmod 33$

$= (71 \times 71 \times 8) \bmod 33$

$= 40328 \bmod 33$

$\boxed{C = 57}$

Decryption :-

$M = C^d \bmod n.$

$= 57^{53} \bmod 77$

$=$

$57 \bmod 77 = 57.$

$57^2 \bmod 77 = 3249 \bmod 77$

$= 15$

$57^4 \bmod 77 = 15 \times 15 \bmod 77$

$= 225 \bmod 77$

$= 71.$

$57^8 \bmod 77 = 57^4 \times 57^4 \bmod 77$

$= (71 \times 71) \bmod 77$

$= 5041 \bmod 77$

$= 36.$

$57^{10} \bmod 77 = (36 \times 35) \bmod 77$

$= 540 \bmod 77$

$= 1.$

$57^{53} \bmod 77 = (1 \times 1 \times 1 \times 1 \times 1 \times 15 \times 57) \bmod 77$

$= 855 \bmod 77$

$= 8$

$\boxed{M = 8}$