1) $p = 7 \quad q = 11 \quad e = 17 \quad M = 8$

$$n = p \times q$$

$$n = 7 \times 11$$

$$n = 77$$

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

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

$$= 6(10)$$

$$= 60$$

$$\phi(n) = 60$$

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

$e = 17 \rightarrow$ Given

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

$$d \equiv 17^{-1} \bmod 60$$

$60 \times 1 = \frac{60+1}{17} = \frac{61}{17} = 3 \neq 0$ (remainder)

$60 \times 2 = \frac{120+1}{17} = \frac{121}{17} = +2 \neq 0$

$60 \times 3 = \frac{180+1}{17} = \frac{181}{17} = 10 \neq 0$

$17\overline{)61}$ → 31, 51, 20, 17, 3

$\times 4$

$\times 5$

$\times 6$

$\times 7$

$\times 8$

$\times 9$

$\times 10$

$\times 11$

$\times 12$

$\times 13$

$\times 14$

$60 \times 15 = \frac{900+1}{17} = 0$ (remainder)

↳ quotient $= 53 = d$

$\therefore d = 53$

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

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

Encryption:-

$$C = M^e \bmod n$$

$C = 8^{17} \bmod 77$

$8^{17} = 8^8 \times 8^8 \times 8$

$8 \bmod 77 = 8$

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

$= 64 \bmod 77$

$= 64$

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

$= (64 \times 64) \bmod 77$

$= 4096 \bmod 77$

$= 15$

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

$= (15 \times 15) \bmod 77$

$= 225 \bmod 77$

$= 71$

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

$= (71 \times 71 \times 8) \bmod 77$

$= 40328 \bmod 77$

$= 57$

$\boxed{C = 57}$

Decryption:

$M = C^d \bmod n$

$= 57^{53} \bmod 77$

$57^{53} = 57^{10} \times 57^{10} \times 57^{10} \times 57^{10} \times 57^{10} \times 57^2 \times 57$

$57 \mod 77 = 57$

$57^2 \mod 77 = (57 \times 57) \mod 77$

$= 3249 \mod 77$

$= 15$

$57^4 \mod 77 = (57^2 \times 57^2) \mod 77$

$= (15 \times 15) \mod 77$

$= 225 \mod 77$

$= 71$

$57^8 \mod 77 = (5^4 \times 5^4) \mod 77$

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

$= 5041 \mod 77$

$= 36$

$57^{10} \bmod 77 = (57^9 \times 57^9) \bmod 77$

$= (36 \times 15) \bmod 77$

$= 540 \bmod 77$

$= 1$

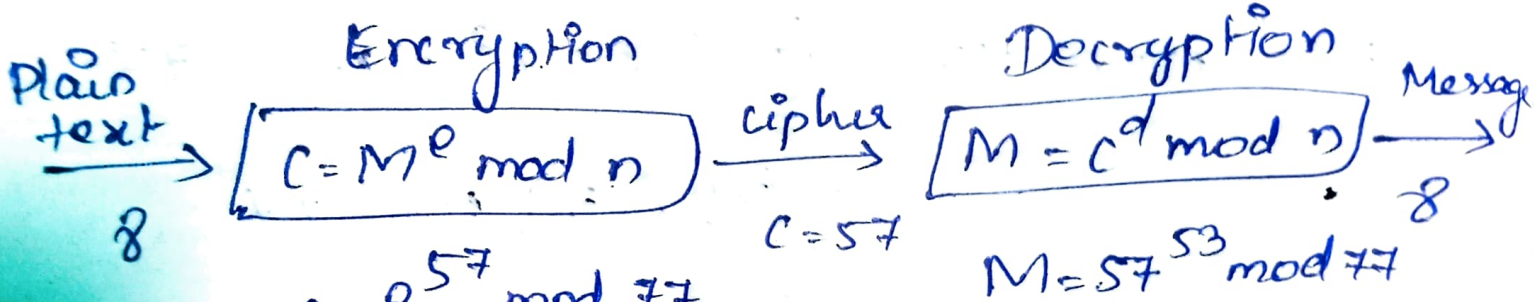
$57^{53} \bmod 77 = (57^{10} \times 57^{10} \times 57^{10} \times 57^{10} \times 57^{10} \times 57^{8} \times 57^{1}) \bmod 77$

$= (1 \times 1 \times 1 \times 1 \times 1 \times 15 \times 57) \bmod 77$

$= 855 \bmod 77$

$= 8$

$M = 8$


Encryption
Decryption
Plain text
8
$C = M^e \bmod n$
$C = 8^{57} \bmod 77$
ciphue
$C = 57$
$M = C^d \bmod n$
$M = 57^{53} \bmod 77$
Message
8