7.3.7 Q7 RSA

$p=3$ $q=7$

(i) 2 first possible public keys e.

(ii) Bob : $d \leftarrow e=5$

(iii) $M=8$. $\rightarrow C$

Solution (i) ① $n = p \times q = 3 \times 7 = 21$

$\phi(n) = (p-1) \times (q-1) = 2 \times 6 = 12$

Factor 2 : 2

6 : 2, 3

prime : 2 3 5 7 9 11

X X ✓ ✓ ✓ ✓

the fire two possible values for public key are 5 and 7

(ii) $d = \frac{k\phi(n)+1}{e}$

$d = \frac{12k+1}{5}$

For $k=1$, $d = \frac{12+1}{5} = \frac{13}{5}$

since the result not a whole number it doesnt satisfy the condition

For $k=2$, we have

$d = \frac{12 \times 2 + 1}{5} = \frac{24+1}{5} = \frac{25}{5} = 5$

Bob's private key = 5

(iii) Encryption in RSA

$C = m^e \bmod n$

$= 8^5 \bmod 21$

$= 8$

The ciphertext $= 8$