7.3.6 Q6. RSA

Q: $p=3$ $q=11$

$e=7$ $M=6$

(i) d

(ii) d s.

(iii) verify

Solution (i) ① $d = \frac{k \cdot \phi(n) + 1}{e}$

$n = p \times q = 3 \times 11 = 33$

$\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$

Factor : $p-1 = 2 : 2$

$q-1 = 10 : 2, 5$

$e = 7$

$d = \frac{20k+1}{7}$

For $k=1$, $d = \frac{20+1}{7} = \frac{21}{7} = 3$

So $d=3$

(ii) $S = M^d \bmod n$

$= 6^3 \bmod 33$

$= 18$

This is digital signature

(iii) $M = S^e \bmod n$

$= 18^7 \bmod 33$

$= 6$

Since Alice is able to recover the

message by decrypting the digital signature using Bob's public key, it is confirmed that it was Bob who has sign it. This verify the digital signature