RSA - revision

Q $p = 5$ $q = 11$

Alice Bob

$e = 3$

$d = ?$

$M = 4$

$C = ?$ $M = ?$

Solution ① $N = p \times q = 5 \times 11 = 55$

$\phi(n) = (p-1) \times (q-1) = 4 \times 10 = 40$

$\gcd(e, \phi(N)) = 1$, $1 < e < \phi(N)$, e is prime

$e = 3$

$e \cdot d = 1 (\text{mod } \phi(N))$

$\frac{ed}{\phi(n)} = k \cdots 1 \Rightarrow d = \frac{k\phi(n)+1}{e}$

$d = \frac{40k+1}{3}$, $1 < d < \phi(n)$

let $k = 1$, $d = \frac{41}{3}$ ✗

$k = 2$, $d = \frac{81}{3} = 27$ ✓

② $C = M^e \bmod N$

$= 4^3 \bmod 55$

$= 9$

③ $M = C^d \bmod H$

$= 9^{27} \bmod 55$

$= 9^{26} \cdot 9 \bmod 55$

$= (9^2)^{13} \cdot 9 \bmod 55$

$= 26^{12} \cdot 26 \cdot 9 \bmod 55$

$= (26^4)^3 \cdot 26 \cdot 9 \bmod 55$

$= 36^3 \cdot 26 \cdot 9 \bmod 55$

$= 4$