7.3.4 Q4 RSA

Q: Jenifer $\xrightarrow[M=24\ ① \leftarrow ?]{p=7\ q=11}$ Ted

$e=13$

$d=37$

② $e=2$ problem

Solution ① $y=24$, $e=13$, $d=37$, $n=77$

$C = y^e \bmod n$

$= 24^{13} \bmod 77$

$= 24^{12} \cdot 24 \bmod 77$

$= (24^3)^4 \cdot 24 \bmod 77$

$= 41^4 \cdot 24 \bmod 77$

$= 52$

Ted will send $C=57$ to Jenifer

② when Jenifor receives the encrypted message 52, she uses her private key $d=37$ to decode it.

$M = C^d \bmod n$

$= 52^{37} \bmod 77$

$= (52^3)^{12} \times 52 \text{ md } 77$

$= 6^{12} \times 52 \text{ md } 77$

$= (6^6)^2 \times 52 \text{ md } 77$

$= 71^2 \times 52 \text{ md } 77$

$= 24$

which in this case is Y

③ If Jenifer choose, publick key $e=2$ then this will not be RSA, because in RSA e (public key) must be ralatively prime to $\phi(n)$ and less than $\phi(n)$

④ Thus, Jenifer cannot choose public key $e=2$, as this will not fulfil the required condition for RSA algorithm.