Assignment 4 Q2

watIAM: sh2yap
Student ID: 21111395

(a) No, because the security of RSA depends on the difficulty of factoring n. If n is just p^2 then we can easily compute the factors by trial divisions. In fact, an attacker can easily factorise by taking $\sqrt{n}$. (square root attack)

(b) Common modulus attack

Bob $\xrightarrow{c_1 = m^{e_1} \bmod n}$ Alice: (n, e_1), p, q $\quad d_{Alice} = e_1^{-1} \bmod \phi(n)$

Bob $\xrightarrow{c_2 = m^{e_2} \bmod n}$ Alicia: (n, e_2), p, q $\quad d_{Alicia} = e_2^{-1} \bmod \phi(n)$

assumption : $\gcd(e_1, e_2) = 1$ —① (since coprime)
and the messages are encrypted using Euclid's algorithm
∴ there exists s_1, s_2 s.t. $e_1 s_1 + e_2 s_2 = 1$ (Bézout's Theorem)

$$
\begin{aligned}
c_1^{s_1} * c_2^{s_2} &= m^{e_1 s_1} * m_2^{e_2 s_2} \bmod n \\
&= m^{e_1 s_1 + e_2 s_2} \bmod n \\
&= m^1 \bmod n \\
&= m \bmod n
\end{aligned}
$$

So all the attacker needs to do is find s_1 and s_2 using Extended Euclidean algorithm and compute $c_1^{s_1} * c_2^{s_2} \bmod n$

Assignment 4 Q2

(c)

$c_1 = m^{e_1} \bmod (pr)$
$= m^{e_1} \bmod N$

Bob $\rightarrow$ Alice (N, e_1) p, r $\qquad d_{Alice} = e_1^{-1} \bmod \phi(n_1)$, $N = pr$

Bob $\rightarrow$ Alicia (M, e_2) p, q $\qquad d_{Alicia} = e_2^{-1} \bmod \phi(n_2)$, $M = pq$

$c_2 = m^{e_2} \bmod (pq)$
$= m^{e_2} \bmod M$

we note that N and M has a gcd of p
$\therefore$ we can use Extended Euclidean algorithm to obtain p.

Once p is obtained, we can factorise get r and q by:

$$r = \frac{N}{p} \quad \text{and} \quad q = \frac{M}{p}$$

this clearly compromises the private keys of both Alice and Alicia, as the attacker has $\phi(n_1)$, $\phi(n_2)$ e_1 and e_2, so the attacker can compute d_{Alice} and d_{Alicia} using modulo inverse!