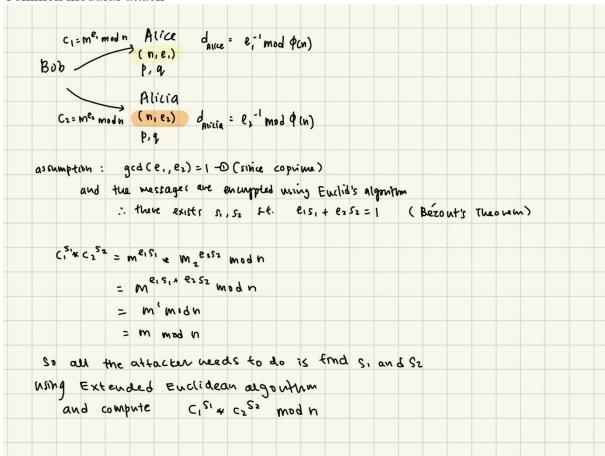
watIAM: sh2yap Student ID: 21111395

- (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



= Me'mod	N Alice	dalice = e	i'mod pan)	, N=pr		
06	p, r	••••				
	Alicio					
Cz= Mez mod	(pq) (M,ez)	d <sub>Avicia</sub> = e	, - 1 mod 4 (n)	M=Pq		
= Mez mod	M P, 9	,,,,,,				
we note	that N	and M	has a g	cd of p		
					gontum	to obtam
þ.			•••••	•••••		
once p	is obtain	red, we	can fac	tonse ge	t r and	9,
•	r = F	and q	, = <del>-</del>			
this c	learly s	im orgmo	zes the	private &	eys of	
					7 /	i), $\phi(nz)$
e, an	9 65 '	so the	attacke	man c	ompute	d mice and
		modula				W. (C