watIAM: sh2yap

Student ID: 21111395

1. No, because the security of RSA depends on the difficulty of factoring n. If n is just p2 then we can easily compute the factors by trial divisions. In fact, an attacker can easily factorise by taking . (square root attack)
2. Common modulus attack

A math equations on a graph paper

Description automatically generated

