MATH V3025: CHINESE REMAINDER THEOREM ATTACK ON RSA FOR HW 4

Suppose that Alice uses RSA to encrypt and send the same message m to Bob, Carl, and Dan. Their RSA public keys are, respectively, $(n_B, e_B), (n_C, e_C)$, and (n_D, e_D), where n_B, n_C, and n_D are relatively prime, but $e_B = e_C = e_D = 3$.

Question 1: Why is $m^3 < n_B n_C n_D$?

Question 2: How can Eve compute m exactly using the Chinese Remainder Theorem, and *without* factoring n_B, n_C, or n_D?

Question 3: Let $n_B = 26$, $n_C = 33$, $n_D = 35$. Eve sees the encrypted messages 25 sent to Bob, 29 sent to Chuck, and 13 sent to Dan. Use the algorithm you found in Question 2 to find m.