CS250/219 Database Systems: Ex 9

Problem 1. Consider an RSA cryptosystem with p = 17, q = 13 (hence, n = pq = 221), and e = 35.

a) What is the value of d?

b) Let (e, n) be the public key of Alice. If we use it to encrypt a message m = 78, what is the ciphertext C?

c) Let (d, n) be the private key of Alice. If she receives a ciphertext C = 65, what is the original message m?

Problem 2. Suppose that Alice's public key is (13, 77). You are a hacker. Suppose that you have intercepted an encrypted message C = 64 for Alice. Now, break RSA by figuring out the original message.