Introduction to mathematical cryptography
Homework problems
Week 8

15. Analyze what happens with RSA if $p = q$: compute $\varphi(N)$, and explain why this setup is not secure.

16. Alice decides to use RSA with the public key $N = 1889570071$. In order to guard against transmission errors, Alice has Bob encrypt his message twice, once using the encryption exponent $e_1 = 1021763679$ and once using the encryption exponent $e_2 = 519424709$. Eve intercepts the two encrypted messages $c_1 = 1244183534$ and $c_2 = 732959706$. Assuming that Eve also knows N and the two encryption exponents e_1 and e_2, help Eve recover Bobs plaintext without finding a factorization of N. (In your solution, you might need euclidean algorithm and modular exponentiation on 10 digit numbers. If you cannot find online tools and cannot write short programs either to execute these calculations, then at least try to describe them as clearly as possible. In this case, you don't have to give the exact numerics.)

Note: Please, provide complete arguments everywhere, and explain how you arrived at your answer/solution. Giving the result without explanation leads to score deduction.