Recitation 7: RSA

(Question 3 in Ex6)

Alice generates a public key and a private key that allows Bob to send an encripted message which she can decript, while others need to factor a number to do so.

Keys: Her public key includes $N = p \cdot q$ for prime numbers p, q and e that is coprime to $\Phi(N)$ (she can draw a number and divide by the GCD with $\Phi(N)$) and her private key is p, q.

Encription: When Bob wants to send the message $a \in [N-1]$, he sends $b := a^e \pmod{N}$.

Decription: When Alice wants to read Bob's message she calculates $b^d \equiv a \pmod{N}$ for $de \equiv 1 \pmod{\Phi(N)}$.

1. What is $\Phi(N)$? How can Alice know it?
2. Show how Euclid's algorithm allows Alice to calculate d efficiently.
3. Show that indeed $b^d = a^{de} \equiv a \pmod{N}$.

   hint: use lagrange's theorem or the Chinese remainder theorem together with Euler's theorem.
4. How could Eve, who already knows the public key N, e and the encripted message b, learn the message itself a if she could factor any number to its prime factors?