MSG-Hausaufgaben Blatt 2

Zum 18.09.2018

Aufgabe 1. Die Zahl $\varphi(n)$ gibt die Anzahl der positiven ganzen Zahlen $\leq n$ die teilerfremd zu n sind an.

a) Berechne $\varphi(24)$, $\varphi(90)$, $\varphi(81)$, $\varphi(91)$.

b) Seien p und q zwei verschiedene Primzahlen. Was ist dann $\varphi(p^3 \cdot q^4)$?

c) Seien p, q und r drei verschiedene Primzahlen. Was ist dann $\varphi(p \cdot q \cdot r)$?

Aufgabe 2. Stelle das RSA-Verschlüsslungsverfahren nach! Du wählst dir am Anfang die beiden Primzahlen $p = 3373$ und $q = 5927$ und den public key $e = 8714785$.

a) Berechne $n = p \cdot q$ und $\varphi(n)$.

b) Überprüfe mit dem Euklidischen Algorithmus, dass $\varphi(n)$ und e teilerfremd sind.

c) Mit dem erweiterten Euklidischen Algorithmus kannst du nun den private key d finden sodass $e \cdot d \equiv 1 \pmod{\varphi(n)}$ ist.

d) Verschlüssle $m = 234173$ indem du $m^e \pmod{n}$ berechnest.

e) Prüfe deine Ergebnisse, indem du die Nachricht mit dem private key entschlüsselst.

Leiter: Anastasia Prokudina (anastasia.prokudina@gmx.de), Simone Zahn
Webseite: https://www2.mathematik.hu-berlin.de/~prokudia/
Ort und Zeit: Rudower Chaussee 25, Raum 1.114, Dienstags 16:00-17:30