Mathe für die Informatik II – SoSe 2018

Dr. Samuel Hetterich

Blatt 2 Abgabe: Do 03.05.2018, 12:15 Uhr

Hinweis:

▶ Bewertet und korrigiert werden nur die Aufgaben 2.1 bis 2.3 - also müssen Sie nur Lösungen dieser Aufgaben einreichen. Die Präsenzaufgaben 2.4 und 2.5 werden in den Tutorien gelöst und besprochen - gerne können Sie sich darauf vorbereiten.

▶ In der Vorlesung wird Ihnen der Gebrauch der freien Software Sage zur Lösung mathematischer Probleme nahegebracht. Diese Software lässt sich hier `www.sagemath.org/download` kostenlos herunterladen. Auf den folgenden Übungsblättern befindet sich nun jeweils eine Sage-Aufgabe. Diese Aufgabe lösen Sie indem Sie Ihren Programmcode und Ihre Berechnungen ausdrucken, an Ihre Abgabe heften und Ihren Programmcode über OLAT/per Mail Ihrem Tutor elektronisch zukommen lassen.

Aufgabe 2.1 — 5 Punkte

a) Für das RSA-Verfahren sei der Modul $\mathsf{N} = p \cdot q$ mit Primfaktoren $p = 17$ und $q = 23$. Berechnen Sie den Dekodierschlüssel der zum Schlüssel $\mathsf{e} = 73$ für den Modul N.

b) Entschlüsseln Sie die (bereits mit e verschlüsselte) Nachricht $m = 4$.

c) Erzeugen Sie zur Nachricht $a = 6$ und den Parametern aus a) eine RSA-Signatur (a, c) und zeigen Sie, dass diese Signatur gültig ist (sich mit Kenntnis von d verifizieren lässt).

d) Wäre $\mathsf{e}' = 23$ für den Modul $\mathsf{N} = 17 \cdot 23$ ein zulässiger öffentlicher Schlüssel? (Begründung!)

Aufgabe 2.2 — 6 Punkte

Es seinen p und q verschiedene Primzahlen.

a) Wieviele mögliche öffentliche Schlüssel gibt es für das RSA-Verfahren mit Modul $\mathsf{N} = p \cdot q$?

b) Zeigen Sie zusätzlich zu a), dass die Anzahl der möglichen öffentlichen Schlüssel e gerade ist.

c) Kann man p und q so wählen, dass es einen geraden öffentlichen Schlüssel e gibt?

Begründen Sie jeweils ihre Aussagen.

Aufgabe 2.3 — 5 Punkte

Schreiben Sie eine Funktion `phirueck_2(a)` in Sage, die für eine Liste von beliebig vielen Faktoren (beispielsweise `a = [2,4,10]` die Schritte 2.1 und 2.2 des in der Vorlesung vorgestellten Schemas zur Rückwärtsberechnung der eulerschen φ-Funktion durchführt. Die Funktion `phirueck_2(a)` soll eine Liste von in Schritt 2.1 und Schritt 2.2 gefundenen Lösungen ausgeben.
Es helfen Ihnen sicherlich die Funktionen `is_prime(n)`, welche prüft, ob `n` eine Primzahl ist und `factor(n)`, welche die Primfaktorzerlegung von n als Liste von Tupeln (Primfaktor und Exponent) liefert. Die Funktion `gcd(n,m)` liefert den größten gemeinsamen Teiler von `n` und `m`.

Präsenzaufgabe 2.4 — 4 Zusatzpunkte

Berechnen Sie:

a) $\mathsf{Rest}(2^{167}, 83)$

b) $\mathsf{Rest}(3^{167}, 17)$

c) $\mathsf{Rest}(12^5, 3)$ (mit Hilfe des kleinen Satzes von Fermat)

d) Berechnen Sie mit Hilfe des Algorithmus SPot (schnelles Potenzieren - 4.3.10 im Skript) die Potenz $a = 11^{14}$ (benutzen Sie für die einzelnen Rechnungen gerne einen Taschenrechner). Wieviele Multiplikationen benötigen Sie dafür?

Präsenzaufgabe 2.5 **4 Zusatzpunkte**

a) Zeigen Sie

$$10^i \equiv (-1)^i \pmod{11} \qquad \text{für } i \geq 0.$$

Wie lässt sich daraus für eine allgemeine Zahl der Rest beim Teilen durch elf errechnen?
Tipp: Was ist $a \cdot 10^2 + b \cdot 10^1 + c \cdot 10^0 \pmod{11}$*?*

b) Zeigen Sie, dass die Zahl 4.531.893.868 keine Quadratzahl ist, indem Sie den Rest modulo 11 betrachten.