Übungen zur Elementaren Zahlentheorie

Wintersemester 2015/16

Prof. Dr. K. Wingberg
O. Thomas

Blatt 4
Abgabe bis 12.11.2015, 11:00h

Aufgabe 13. *(2+2 Punkte)*
Seien p und q verschiedene ungerade Primzahlen, $n = pq$, $1 < e < \phi(n)$ eine natürliche Zahl teilerfremd zu $\phi(n)$ und $1 < d < \phi(n)$ die eindeutig bestimmte natürliche Zahl mit $de \equiv 1 \mod \phi(n)$. Betrachte die Abbildungen

$$\mathrm{ENC}_{(n,e)} \colon \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto x^e$$

und

$$\mathrm{DEC}_{(n,d)} \colon \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto x^d.$$

Man nennt das Paar (n, d) den *geheimen Schlüssel*, der zum *öffentlichen Schlüssel* (n, e) gehört.

(i) Es ist $\mathrm{DEC}_{(n,d)} \circ \mathrm{ENC}_{(n,e)} = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$.

(ii) Es heißt, dass (bei sinnvoller Wahl von p, q und e) es sich hierbei um ein *sicheres* Verschlüsselungsverfahren handelt, d. h. unter anderem, dass aus dem Paar (n, e) nur unter großer Anstrengung das Paar (n, d) rekonstruiert werden kann. Wie würde man naiv aus (n, e) das Tupel (n, d) berechnen und worin liegt die Schwierigkeit? Wieso ist das bei der ersten Berechnung von (n, d) kein Problem?

Aufgabe 14. *(4·2 Punkte)*
Emmy und Fritz möchten geheime Nachrichten unter den Augen ihres Vaters Max austauschen, ohne, dass dieser die Nachrichten versteht. Sie einigen sich darauf, den Buchstaben „A“ mit der Zahl 10 zu kodieren, „B“ mit der Zahl 11, …, „Z“ mit der Zahl 35.

(i) Emmy sucht sich die Primzahlen 83 und 43 aus. Als e wählt sie die kleinste mögliche Zahl ≥ 40. Wie lautet d? Man benutze hierfür den euklidischen Algorithmus.

(ii) Fritz findet einen Zettel von Emmy, in welchem sie ihm (n, e) mitteilt. Er kodiert die Nachricht „BIER“, indem er nacheinander das Buchstabenpaar „BI“ und „ER“ verschlüsselt. Hierbei wird etwa das Buchstabenpaar „AA“ zu 1010, „AB“ zu 1011, „AZ“ zu 1035 etc. Welche Zahlen übermittelt er Emmy?

(iii) Man vollziehe nach, wie Emmy diese Nachricht entschlüsselt.

(iv) Fritz lässt sein eigenes Paar (n', e') auf dem Frühstückstisch liegen, es lautet $(4331, 11)$. Als Max die Nachricht von Emmy an Fritz mit dem Inhalt $(2453, 1829, 1321)$ abfängt, versucht er sie zu entschlüsseln. Wie lautet sie?

Aufgabe 15. *(6 Punkte)*
Es gibt unendlich viele Primzahlen kongruent 1 modulo 6.

Aufgabe 16. *(3+3 Punkte)*

(i) Bestimme alle Primitivwurzeln modulo 11.

(ii) 4 ist niemals eine Primitivwurzel in $\mathbb{Z}/p\mathbb{Z}$ für p prim.