# Diskrete Mathematik ICE

6. Übungsblatt

3. Mai 2016

In allen verschlüsselten Texten wurde die Konvention von Seite A.27 aus dem Skript verwendet. Die Buchstaben werden dabei paarweise in Zahlen übersetzt wie im Folgenden am Beispiel `XL` gezeigt. `X` ist der 24. Buchstabe im Alphabet und `L` der 12. Buchstabe. Das Paar `XL` wird in die Zahl

$$(24-1)\cdot 26 + (12-1) = 609$$

übersetzt.

**26.** Die Zahlenfolge $(515, 544, 100, 330)$ wurde mit dem RSA-Algorithmus mit dem öffentlichen Schlüssel $m = 697$ und $r = 587$ verschlüsselt. Ermitteln Sie den privaten Schlüssel $s$ und entschlüsseln Sie die Nachricht. Rechnen Sie beim Entschlüsseln wie gewohnt modulo $m$ (und nicht modulo $p$ und $q$ wie in Aufgabe 28).

**27.** Alice hat für den RSA-Algorithmus den öffentlichen Schlüssel $m = 667$ und $r = 507$ bekannt gegeben. Sie schickt nun die Nachricht `SIGNATUR` im Klartext und dazu die verschlüsselte Zahlenfolge $(568, 123, 617, 77)$. Entschlüsseln Sie diese Zahlenfolge mit Hilfe des öffentlichen Schlüssels. Mit welchem Schlüssel hat Alice die Zahlenfolge verschlüsselt? Rechnen Sie beim Entschlüsseln wie gewohnt modulo $m$ (und nicht modulo $p$ und $q$ wie in Aufgabe 28).

**28.** Die Entschlüsselung beim RSA-Algorithmus kann effizienter gestaltet werden, wenn man anstatt $g(y) = y^s \bmod m$ zunächst $g_p(y) = y^s \bmod p$ und $g_q(y) = y^s \bmod q$ berechnet und dann $g(y)$ mit Hilfe des chinesischen Restsatzes aus $g_p(y)$ und $g_q(y)$ bestimmt. Führen Sie dieses Prinzip für die Entschlüsselungen aus den Aufgaben 26 und 27 durch.

**29.** Seien $m, r, s \in \mathbb{N}$ mit $rs \equiv 1 \bmod \varphi(m)$.

(a) Zeigen Sie, dass $a^{rs} \equiv a \bmod m$ für alle $a \in \mathbb{N}$ gilt (und $m, r, s$ somit als RSA-Schlüssel dienen könnten), falls

$$a^{\varphi(m)+1} \equiv a \bmod m \qquad \text{für alle } a \in \mathbb{N}. \tag{1}$$

(b) Zeigen Sie, dass $m$ die Eigenschaft (1) erfüllt, falls $m$ das Produkt lauter verschiedener Primzahlen $p_1, p_2, \ldots, p_n$ ist. (*Hinweis:* Betrachten Sie $a^{\varphi(m)+1} \bmod p_i$ für jedes $i$ separat.) Zeigen Sie umgekehrt, dass (1) nicht für alle $a \in \mathbb{N}$ erfüllt ist, sobald es eine Primzahl $p$ gibt, deren Quadrat $p^2$ ein Teiler von $m$ ist.

**30.** Erstellen Sie die Wahrheitstafeln für die Formeln

$$\Big((A \vee B) \wedge \big((\neg B) \wedge C\big)\Big), \qquad \big((A \leftrightarrow B) \leftrightarrow C\big) \qquad \text{und} \qquad \big(A \leftrightarrow (B \leftrightarrow C)\big).$$