Aufgabe 29. Erstelle ein Schema des Diffie-Hellman-Merkle-Schlüsselaustauschs für drei Teilnehmer, sodaß am Ende alle drei Teilnehmer den gleichen Schlüssel haben. Wieviele Botschaften müssen dafür mindestens ausgeschickt werden?

Aufgabe 30. (a) Berechne die Eulersche Funktion $\varphi(m)$ für die Zahl $m = 7371$.
(b) Zeige, daß $a^{\varphi(81)+1} \not\equiv a \mod 81$ genau dann gilt, wenn $\mathrm{ggT}(a, 81) \in \{3, 9, 27\}$.
(c) Zeige, daß $a^{\varphi(7371)+1} \not\equiv a \mod 7371$ genau dann gilt, wenn $\mathrm{ggT}(a, 81) \in \{3, 9, 27\}$.
Hinweis: Chinesischer Restsatz!

Aufgabe 31. Sei $m = pq$ und $\mathrm{ggT}(r, \varphi(m)) = 1$. Aus dem euklidischen Algorithmus folgt, daß es ein $s \in \mathbb{Z}$ gibt sodaß $rs \equiv 1 \mod \varphi(m)$. Warum stimmt die Behauptung aus der Vorlesung, daß immer $s \in \mathbb{N}$, d.h. $s > 0$, gewählt werden kann?

Aufgabe 32. Gegeben sei $m = 1247$.
(a) Welche der folgenden Zahlen sind als öffentliche RSA-Schlüssel geeignet (Begründung!)?

$$r = 41 \qquad r = 42 \qquad r = 43$$

Berechne die zugehörigen inversen Schlüssel.
(b) Wähle einen geeigneten Schlüssel und verschlüssle die Botschaft

"WOWOAMEILEISTUNG"

mit der Konvention aus der Vorlesung (Bsp (10.7)).
(c) Erstelle eine digitale Signatur für die Nachricht

"FAKENEWS"

(d) Die folgende Nachricht wurde mit dem Schlüssel $r = 17$, $m = 1247$ verschlüsselt.

$$[496, 361, 492, 1217, 226, 821, 486, 164, 516]$$

Finde den inversen Schlüssel s und entschlüssle die Botschaft.

Hinweis: Für die Zwischenrechnungen ist ein Computer erlaubt.

Aufgabe 33. Die Ver- und Entschlüsselungen beim RSA-Verfahren können effizienter gestaltet werden, wenn man die Potenzfunktionen $e_m(x, k) = x^k \mod m$ zunächst die Funktionen $e_p(x, k) = x^k \mod p$ und $e_q(x, k) = x^k \mod q$ berechnet und dann das Ergebnis mit Hilfe des chinesischen Restsatzes ermittelt. Verwende dieses Prinzip, um die folgende Aufgabe ohne elektronische Hilfsmittel zu lösen:
Für den RSA-Algorithmus wurde der öffentliche Schlüssel $m = 91$ und $r = 13$ bekanntgegeben.
(a) Verschlüssle die Nachricht $(14, 42)$.
(b) Berechne den Geheimschlüssel s.
(c) Berechne eine digitale Signatur für die Nachricht $(33, 5)$.