Aufgabe 36. Erstelle ein Schema des Diffie-Hellman-Merkle-Schlüsselaustauschs für drei Teilnehmer, sodaß am Ende alle drei Teilnehmer den gleichen Schlüssel haben. Wie kann man die ausgetauschten Botschaften so bündeln, daß möglichst wenige Kontakte getätigt werden müssen?

Führe den Austausch anhand des Beispiels $p = 41$, $g = 11$, $a = 11$, $b = 12$, $c = 13$ durch (Computer erlaubt).

Aufgabe 37. (a) Berechne die Eulersche Funktion $\varphi(m)$ für die Zahl $m = 6885$.
(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 $a^{\varphi(6885)+1} \not\equiv a \mod 6885$ genau dann gilt, wenn $\mathrm{ggT}(a, 81) \in \{3, 9, 27\}$.
Hinweis: Chinesischer Restsatz!
(d) Überprüfe diese Tatsachen am Computer für $a \in \{1, 2, \ldots, 6885\}$.

Aufgabe 38. Gegeben sei $m = 1333$.
(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

"FAKENEWS"

mit der Konvention aus der Vorlesung (Bsp (11.7); ohne Störzeichen).
(c) Die folgende Nachricht wurde mit dem Schlüssel $r = 17$, $m = 1333$ verschlüsselt.

$$[367, 490, 535, 658, 1129, 133, 787, 293, 301]$$

Finde den inversen Schlüssel s und entschlüssle die Botschaft.

Hinweis: Für die Zwischenrechnungen ist ein Computer erlaubt.

Aufgabe 39. 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 $m = 85$ und $r = 13$ bekanntgegeben.
(a) Verschlüssle die Nachricht $(14, 42)$.
(b) Berechne den Geheimschlüssel s und entschlüssle die Botschaft.

Aufgabe 40. Begründe, warum im RSA-Verfahren anstelle von $\phi(m) = (p-1)(q-1)$ auch die Zahl $\lambda(m) = \mathrm{kgV}(p-1, q-1)$ verwendet werden kann.

Hinweis: Chinesischer Restsatz!