Aufgabe 33. 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 34. Gegeben sei $m = 1363$.

(a) Welche der folgenden Zahlen sind als öffentliche RSA-Schlüssel geeignet (Begründung!)?

$$r = 21 \qquad r = 23 \qquad r = 25$$

Berechne die zugehörigen inversen Schlüssel.

(b) Wähle einen geeigneten Schlüssel und verschlüssle die Botschaft

"FAKENEWS"

mit der Konvention aus der Vorlesung (Bsp (11.8); ohne Störzeichen).

(c) Die folgende Nachricht wurde mit dem Schlüssel $r = 17$, $m = 1363$ verschlüsselt.

$$[579, 304, 816]$$

Finde den inversen Schlüssel s und entschlüssle die Botschaft.

Hinweis: Für die Zwischenrechnungen ist ein Computer erlaubt.

Aufgabe 35. 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 $m = 119$ und $r = 13$ bekanntgegeben.

(a) Verschlüssle die Nachricht $(14, 42)$.

(b) Berechne den Geheimschlüssel s und entschlüssle die Botschaft.

(c) Berechne eine digitale Signatur für die Nachricht $(33, 5)$.

Aufgabe 36. 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!

Aufgabe 37. Das folgende Beispiel illustriert, daß die Wahl kleiner Schlüssel die Sicherheit des RSA-Verfahrens verringert.

Tom schickt die gleiche Botschaft an seine Freunde Basti, Siggi und Wolfi, die ihm vorher die öffentlichen Schlüssel $(m_1 = 1003, r_1 = 3)$, $(m_2 = 1081, r_2 = 3)$ und $(m_3 = 1189, r_3 = 3)$ bekanntgegeben haben. Die drei verschlüssleten Botschaften sind jeweils $y_1 = (38, 163, 327)$, $y_2 = (426, 955, 989)$ und $y_3 = (891, 728, 144)$. Entschlüssle die Botschaft, ohne die Primfaktorzerlegung der Schlüssel m_i durchzuführen (Computer oder Taschenrechner für Zwischenrechnungen ist zugelassen).

Aufgabe 38. Überprüfe anhand von Wahrheitstafeln, ob die folgenden Aussageformen äquivalent sind:

(a) $(A \to B) \to C$ und $A \to (B \to C)$

(b) $(\neg A \to B) \to (B \vee C)$ und $(A \to B) \vee C$.