Aufgabe 34. Das folgende Beispiel ist mit der Methode aus Aufgabe 33 zu lösen.
Für den RSA-Algorithmus wurde der öffentliche Schlüssel $m = 91$ und $r = 11$ bekanntgegeben.

(a) Verschlüssle die Nachricht $(12, 42)$.
(b) Berechne den Geheimschlüssel s.
(c) Berechne eine digitale Signatur für die Nachricht $(33, 5)$.

Aufgabe 35. Das folgende Beispiel illustriert, daß die Wahl kleiner Schlüssel die Sicherheit des RSA-Verfahrens verringert.
Bob schickt die gleiche Botschaft an seine Freundinnen Alice, Angela und Adina, die ihm vorher die öffentlichen Schlüssel $(m_1 = 1219, r_1 = 3)$, $(m_2 = 799, r_2 = 3)$ und $(m_3 = 1189, r_3 = 3)$ bekanntgegeben haben. Die drei Botschaften sind $y_1 = (108, 1117, 317)$, $y_2 = (210, 220, 88)$ und $y_3 = (657, 1029, 831)$. Entschlüssle die Botschaft, ohne die Primfaktorzerlegung der Schlüssel m_i durchzuführen (Computer oder Taschenrechner für Zwischenrechnungen ist zugelassen).

Aufgabe 36. Überprüfe anhand von Wahrheitstafeln, für welche Belegungen die folgenden Aussageformen erfüllt sind sind:

(a) $A \vee (C \to (B \wedge (A \wedge (\neg(A \leftrightarrow (B \vee C))))))$

(b) $(((((A \vee C) \to B) \wedge A) \wedge (\neg A)) \leftrightarrow C) \vee B$

Aufgabe 37. Alice, Bob und Charles sind zu einer Geburtstagsfeier eingeladen. Wie das bei den Leuten so ist, haben alle Vorbehalte:

(a) Wenn Alice nicht kommt, dann kommt auch Bob nicht.
(b) Entweder Bob oder Alice kommt, aber nicht beide.
(c) Charles und Alice kommen, wenn sie kommen, nur zusammen.

Formalisiere die Aussagen und stelle fest, wer zur Feier kommt.

Aufgabe 38. Der Kommissar befragt die Verdächtigen Alice, Bob und Charles für eine Tat. Jede Person lügt einmal und sagt einmal die Wahrheit.

Alice sagt: Ich war es nicht. Ich weiß, daß Charles es getan hat.
Bob sagt: Ich war es nicht. Alice hat es getan.
Charles sagt: Ich war es nicht. Alice weiß nicht, wer es war.

Wer hat es getan?