Aufgabe 28. (a) Berechne die Eulersche Funktion $\varphi(m)$ für die Zahl $m = 9625$.
(b) Zeige, daß $a^{\varphi(m)+1} \not\equiv a \mod m$ genau dann gilt, wenn $\mathrm{ggT}(a, 125) \in \{5, 25\}$.
Hinweis: Chinesischer Restsatz! (2+4P.)

Aufgabe 29. Die Zahlenfolge $(1214, 124, 934, 168)$ wurde mit dem RSA-Algorithmus mit öffentlichem Schlüssel

$$(m = 1247, r = 761)$$

verschlüsselt.
Finde den privaten Schlüssel s und entschlüssle die Nachricht (Die Buchstaben sind paarweise mit der Konvention aus der Vorlesung codiert). (3P.)

Aufgabe 30. 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? (2P.)

Aufgabe 31. 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 $(m_1 = 901, r_1 = 3)$, $(m_2 = 1081, r_2 = 3)$ und $(m_3 = 1189, r_3 = 3)$ bekanntgegeben haben. Die drei Botschaften sind $y_1 = (434, 606, 552)$, $y_2 = (879, 980, 373)$ und $y_3 = (757, 1175, 914)$. Entschlüssle die Botschaft, ohne die Primfaktorzerlegung der Schlüssel m_i durchzuführen (Computer oder Taschenrechner für Zwischenrechnungen ist zugelassen). (3P.)

Aufgabe 32. Im folgenden verschlüsselten Text wurde je ein Caesar-Schlüssel für die Buchstaben an geraden und ungeraden Stellen verwendet:

DJELYNDNZWVWCNTQKBLWUAZWBBBJEWDJE
WZLYCMNCFVLYBVAEFVATQVRERCUKDD

(Leerzeichen wurden entfernt und sind nicht Teil des Alphabets) (2P.)