Aufgabe 42. Um Frequenzanalyse zu erschweren, empfiehlt es sich, Buchstabengruppen zu verschlüsseln, z.B. paarweise. Dazu numeriert man die Buchstaben A-Z von 0 bis 25 durch und faßt diese Zahlen als Ziffern in einem Zahlensystem zur Basis 26 auf. Das heißt, unser "Alphabet" besteht aus $26 \cdot 26 = 676$ Buchstabenpaaren:

$$\begin{array}{llll} AA \triangleq 0, & AB \triangleq 1, & AC \triangleq 2, & \dots \quad AZ \triangleq 25 \\ BA \triangleq 26, & BB \triangleq 27, & BC \triangleq 28, & \dots \quad BZ \triangleq 51 \\ CA \triangleq 52, & CB \triangleq 53, & CC \triangleq 54, & \dots \quad CZ \triangleq 87 \\ \vdots & & & \\ ZA \triangleq 650, & ZB \triangleq 651, & ZC \triangleq 652 & \dots \quad ZZ \triangleq 675, \end{array}$$

d.h. dem Buchstabenpaar $b_i b_j$ entspricht die Zahl $i \cdot 26 + j$
Mit diesen Zahlen kann dann weitergerechnet werden, indem z.B. ein Caesar-Schlüssel modulo 676 addiert wird.

(a) Stelle das Wort OKAY mit diesem Zahlencode dar, addiere dazu den Caesar-Schlüssel 84 und wandle den erhaltenen Code in ein verschlüsseltes Wort um.
(b) Entschlüssle das Wort EURSHX mit dem inversen Schlüssel.

Aufgabe 43. (a) Beschreibe und berechne einen Diffie-Hellman-Schlüsselaustausch mit den Parametern $p = 31$, $g = 7$, $a = 13$, $b = 11$.
(b) Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$\begin{array}{ll} g = 8 & p = 29 \\ m = 10 & n = 16 \end{array}$$

Bestimme die geheimen Parameter a, b und den Schlüssel r!

Aufgabe 44. Welche der folgenden Zahlen g, m, n, p sind für eine Schlüsselvereinbarung nach Diffie-Hellman-Merkle geeignet? Berechne gegebenenfalls die geheimen Parameter a und b sowie den Schlüssel s. (Für die Zwischenrechnungen ist ein Computer erlaubt.)

(a) $g = 17$, $m = 29$, $n = 59$, $p = 201$
(b) $g = 10$, $m = 29$, $n = 45$, $p = 199$
(c) $g = 10$, $m = 24$, $n = 6$, $p = 101$

Aufgabe 45. 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 Aufgabe42.
(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 46. 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 47. In diesem Beispiel soll gezeigt werden, dass die Verwendung kleiner Exponenten in öffentlichen Schlüsseln (z.B. aus Effizienzgründen) problematisch sein kann.
Sei $r = 3$ und es sei bekannt, dass die gleiche Nachricht x mit den öffentlichen Schlüsseln $(m_1, r) = (143, 3)$, $(m_2, r) = (391, 3)$ und $(m_3, r_3) = (899, 3)$ zu folgenden Werten verschlüsselt wurde:

$$x^3 \equiv 129 \mod 143$$
$$x^3 \equiv 281 \mod 391$$
$$x^3 \equiv 380 \mod 899$$

Bestimme x, ohne die Schlüssel m_i zu faktorisieren. Wie groß darf x sein, damit diese Methode funktioniert?

Aufgabe 48. 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!