Lösungen der Übungsaufgaben

17

Übung 1.1
Sei $z = \lfloor \alpha \rfloor = \max\{x \in \mathbb{Z} : x \leq \alpha\}$. Dann ist $\alpha - z \geq 0$. Außerdem ist $\alpha - z < 1$, denn wäre $\alpha - z \geq 1$, dann wäre $\alpha - (z+1) \geq 0$ im Widerspruch zur Maximalität von α. Insgesamt ist also $0 \leq \alpha - z < 1$ oder $\alpha - 1 < z \leq \alpha$. Da es aber in diesem Intervall nur eine ganze Zahl gibt, ist z diese eindeutig bestimmte Zahl.

Übung 1.3
Die Teiler von 195 sind ± 1, ± 3, ± 5, ± 13, ± 15, ± 39, ± 65, ± 195.

Übung 1.5
$1243 \bmod 45 = 28$, $-1243 \bmod 45 = 17$.

Übung 1.7
Angenommen, m teilt die Differenz $b - a$. Sei $a = q_a m + r_a$ mit $0 \leq r_a < m$ und sei $b = q_b m + r_b$ mit $0 \leq r_b < m$. Dann ist $r_a = a \bmod m$ und $r_b = b \bmod m$. Außerdem ist

$$b - a = (q_b - q_a)m + (r_b - r_a). \tag{17.1}$$

Weil m ein Teiler von $b - a$ ist, folgt aus (17.1), dass m auch ein Teiler von $r_b - r_a$ ist. Weil aber $0 \leq r_b, r_a < m$ ist, gilt

$$-m < r_b - r_a < m.$$

Weil m ein Teiler von $r_b - r_a$ ist, folgt daraus $r_b - r_a = 0$, also $a \bmod m = b \bmod m$.

Sei umgekehrt $a \bmod m = b \bmod m$. Wir benutzen dieselben Bezeichnungen wie oben und erhalten $b - a = (q_b - q_a)m$. Also ist m ein Teiler von $b - a$.

J. Buchmann, *Einführung in die Kryptographie*, Springer-Lehrbuch,
DOI 10.1007/978-3-642-39775-2_17

Übung 1.8
Es gilt $225 = 128+64+32+1 = 2^7+2^6+2^5+2^0$. Also ist 11100001 die Binärdarstellung von 225. Die Hexadezimaldarstellung gewinnt man daraus, indem man von hinten nach vorn die Binärdarstellung in Blöcke der Länge vier aufteilt und diese als Ziffern interpretiert. Wir bekommen also 1110 0001, d. h. $14 * 16 + 1$. Die Ziffern im Hexadezimalsystem sind $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$. Damit ist E1 die Hexadezimaldarstellung von 225.

Übung 1.11
1. Die Ereignisse S und $\emptyset$ schließen sich gegenseitig aus. Daher gilt $1 = \Pr(S) = \Pr(S \cup \emptyset) = \Pr(S) + \Pr(\emptyset) = 1 + \Pr(\emptyset)$. Daraus folgt $\Pr(\emptyset) = 0$.
2. Setze $C = B \setminus A$. Dann schließen sich die Ereignisse A und C gegenseitig aus. Damit ist $\Pr(B) = \Pr(A \cup C) = \Pr(A) + \Pr(C)$. Da $\Pr(C) \geq 0$ ist, folgt $\Pr(B) \geq \Pr(A)$.

Übung 1.13
Mit K bezeichne Kopf und mit Z Zahl. Dann ist die Ergebnismenge {KK,ZZ,KZ,ZK}. Die Wahrscheinlichkeitsverteilung ordnet jedem Elementarereignis die Wahrscheinlichkeit $1/4$ zu. Das Ereignis „wenigstens eine Münze zeigt Kopf“ ist {KK,KZ,ZK}. Seine Wahrscheinlichkeit ist $3/4$.

Übung 1.14
Das Ereignis „beide Würfel zeigen ein verschiedenes Ergebnis“ ist $A = \{12, 13, 14, 15, 16, 17, 18, 19, 21, 13, \ldots, 65\}$. Seine Wahrscheinlichkeit ist $5/6$. Das Ereignis „die Summe der Ergebnisse ist gerade“ ist $\{11, 13, 15, 22, 24, 26, \ldots, 66\}$. Seine Wahrscheinlichkeit ist $1/2$. Der Durchschnitt beider Ereignisse ist $\{13, 15, 24, 26, \ldots, 64\}$. Seine Wahrscheinlichkeit ist $1/3$. Die Wahrscheinlichkeit von A unter der Bedingung B ist damit $2/3$.

Übung 1.16
Wir wenden das Geburtstagsparadox an. Es ist $n = 10^4$. Wir brauchen also $k \geq (1 + \sqrt{1 + 8 * 10^4 * \log 2})/2 \geq 118,2$ Leute.

Übung 1.17
Die entsprechende Zufallsvariable ist $\mathbb{Z}_6 \times \mathbb{Z}_6 \to \mathbb{R}$, $(x, y) \mapsto xy$. Jedes Elementarereignis hat die Wahrscheinlichkeit $1/36$. Also ergibt sich der Erwartungswert durch Aufsummieren der Produkte xy für alle $(x, y) \in \mathbb{Z}_6 \times \mathbb{Z}_6$ und Division durch 36. Das Ergebnis ist $12,25$.

Übung 1.18
Wir müssen zeigen, dass es positive Konstanten B und C gibt mit der Eigenschaft, dass für alle $n > B$ gilt $f(n) \leq C n^d$. Man kann z. B. $B = 1$ und $C = \sum_{i=0}^{d} |a_i|$ wählen.

Übung 1.20
Der Algorithmus berechnet zunächst die Bitlänge n von $d-1$. Dann konstruiert er zufällig und gleichverteilt eine n-Bit-Zahl r. Um die Erfolgswahrscheinlichkeit abzuschätzen, müssen wir die Wahrscheinlichkeit dafür bestimmen, dass $r < d$ ist. Sei dazu

$$d = \sum_{i=0}^{n-1} b_i 2^i \tag{17.2}$$

mit den binären Ziffern $b_i \in \mathbb{Z}_2$, $0 \leq i \leq n-1$. Dann ist $b_{n-1} = 1$, weil n die binäre Länge von d ist. Wenn der Koeffizient von 2^{n-1} in der Binärentwicklung von r den Wert 0 hat, ist der Algorithmus erfolgreich. Die Wahrscheinlichkeit dafür ist $1/2$. Damit ist die Erfolgswahrscheinlichkeit des Algorithmus random mindestens $1/2$.

Übung 1.21
Sei d die Eingabe von Algorithmus 1.2. Setze $n = \lfloor \log_2 d \rfloor + 1$. Der Algorithmus durchläuft die for-Schleife n-mal. In jedem Durchlauf führt der Algorithmus eine Verdopplung und eine Addition aus. Die Operanden sind kleiner als $2^n \leq 2d$. Außerdem wirft der Algorithmus einmal eine Münze. Damit hat jeder Durchlauf die Laufzeit $O((\log d)^2)$. Insgesamt hat der Algorithmus also die Laufzeit $O((\log d)^3)$.

Übung 1.22
1. Jeder Teiler von $a_1, \ldots, a_k$ ist auch ein Teiler von a_1 und $\gcd(a_2, \ldots, a_k)$ und umgekehrt. Daraus folgt die Behauptung.
2. Die Behauptung wird durch Induktion über k bewiesen. Für $k = 1$ ist sie offensichtlich korrekt. Sei also $k > 1$ und gelte die Behauptung für alle $k' < k$. Dann gilt $\gcd(a_1, \ldots, a_k)\mathbb{Z} = a_1\mathbb{Z} + \gcd(a_2, \ldots, a_k)\mathbb{Z} = a_1\mathbb{Z} + a_2\mathbb{Z} + \ldots + a_k\mathbb{Z}$ nach 1., Theorem 1.5 und der Induktionsannahme.
3. und 4. werden analog bewiesen.
5. Diese Behauptung wird mittels Korollar 1.3 durch Induktion bewiesen.

Übung 1.24
Wir wenden den erweiterten euklidischen Algorithmus an und erhalten folgende Tabelle

k	0	1	2	3	4	5	6
r_k	235	124	111	13	7	6	1
q_k		1	1	8	1	1	
x_k	1	0	1	1	9	10	19
y_k	0	1	1	2	17	19	36

Damit ist $\gcd(235, 124) = 1$ und $19 * 235 - 36 * 124 = 1$.

Übung 1.26
Wir verwenden die Notation aus dem erweitern euklidischen Algorithmus. Es gilt $S_0 = T_{n+1}$ und daher $x_{n+1} = u_1$ und $y_{n+1} = u_0$. Weiter ist S_n die Einheitsmatrix, also insbesondere $u_n = 1 = r_n/\gcd(a,b)$ und $u_{n+1} = 0 = r_{n+1}/\gcd(a,b)$. Schließlich haben wir in (1.28) gesehen, dass die Folge (u_k) derselben Rekursion genügt wie die Folge (r_k). Daraus folgt die Behauptung.

Übung 1.28
Die Bruchdarstellung einer rationalen Zahl $\neq 0$ ist eindeutig, wenn man verlangt, dass der Nenner positiv und Zähler und Nenner teilerfremd sind. Es genügt daher, zu zeigen, dass der euklidische Algorithmus angewandt auf a, b genauso viele Iterationen braucht wie der euklidische Algorithmus angewandt auf $a/\gcd(a,b), b/\gcd(a,b)$. Das folgt aber aus der Konstruktion.

Übung 1.30
Nach Korollar 1.2 gibt es x, y, u, v mit $xa + ym = 1$ und $ub + vm = 1$. Daraus folgt $1 = (xa + ym)(ub + vm) = (xu)ab + m(xav + yub + yvm)$. Dies impliziert die Behauptung.

Übung 1.32
Ist n zusammengesetzt, dann kann man $n = ab$ schreiben mit $a, b > 1$. Daraus folgt $\min\{a,b\} \leq \sqrt{n}$. Weil nach Theorem 1.6 dieses Minimum einen Primteiler hat, folgt die Behauptung.

Übung 2.1
Einfache Induktion.

Übung 2.3
Wenn e und e' neutrale Elemente sind, gilt $e = e'e = e'$.

Übung 2.5
Wenn e neutrales Element ist und $e = ba = ac$ ist, dann folgt $b = be = b(ac) = (ba)c = c$.

Übung 2.7
Es gilt $4 * 6 \equiv 0 \equiv 4 * 3 \mod 12$, aber $6 \not\equiv 3 \mod 12$.

Übung 2.9
Sei R ein kommutativer Ring mit Einselement e und bezeichne R^* die Menge aller invertierbaren Elemente in R. Dann ist $e \in R^*$. Seien a und b invertierbar in R mit Inversen a^{-1} und b^{-1}. Dann gilt $aba^{-1}b^{-1} = aa^{-1}bb^{-1} = e$. Also ist $ab \in R^*$. Außerdem hat jedes Element von R^* definitionsgemäß ein Inverses.

Übung 2.11
Sei $g = \gcd(a, m)$ ein Teiler von b. Setze $a' = a/g$, $b' = b/g$ und $m' = m/g$. Dann ist $\gcd(a', m') = 1$. Also hat nach Theorem 2.3 die Kongruenz $a'x' \equiv b' \bmod m'$ eine mod m' eindeutig bestimmte Lösung. Sei x' eine solche Lösung. Dann gilt $ax' \equiv b \bmod m$. Für alle $y \in \mathbb{Z}$ erhält man daraus $a(x' + ym') = b + a'ym \equiv b \bmod m$. Daher sind alle $x = x' + ym'$, $y \in \mathbb{Z}$ Lösungen der Kongruenz $ax \equiv b \bmod m$. Wir zeigen, dass alle Lösungen so aussehen. Sei x eine Lösung. Dann ist $a'x \equiv b' \bmod m'$. Also ist $x \equiv x' \bmod m'$ nach Theorem 2.3 und das beendet den Beweis.

Übung 2.13
Die invertierbaren Restklassen mod 25 sind $a + 25\mathbb{Z}$ mit $a \in \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$.

Übung 2.14
Seien a und b ganze Zahlen ungleich Null. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass beide positiv sind. Die Zahl ab ist Vielfaches von a und b. Also gibt es ein gemeinsames Vielfaches von a und von b. Da jedes solche gemeinsame Vielfache wenigstens so groß wie a ist, gibt es ein kleinstes gemeinsames Vielfaches. Das ist natürlich eindeutig bestimmt.

Übung 2.15
Induktion über die Anzahl der Elemente in X. Hat X ein Element, so hat Y auch ein Element, nämlich das Bild des Elementes aus X. Hat X n Elemente und ist die Behauptung für $n-1$ gezeigt, so wählt man ein Element $x \in X$ und entfernt x aus X und $f(x)$ aus Y. Dann wendet man die Induktionsvoraussetzung an.

Übung 2.16
Die Untergruppe ist $\{a + 17\mathbb{Z} : a = 1, 2, 4, 8, 16, 15, 13, 9\}$.

Übung 2.18

a	2	4	7	8	11	13	14
$\operatorname{ord} a + 15\mathbb{Z}$	4	2	4	4	2	4	2

Übung 2.20
Wir zeigen zuerst, dass alle Untergruppen von G zyklisch sind. Sei H eine solche Untergruppe. Ist sie nicht zyklisch, so sind alle Elemente in H von kleinerer Ordnung als $|H|$. Nach Theorem 2.10 gibt es für jeden Teiler e von $|G|$ genau $\varphi(e)$ Elemente der Ordnung d in G, nämlich die Elemente g^{xd} mit $1 \le x \le |G|/d$ und $\gcd(x, |G|/d) = 1$. Dann folgt aber aus Theorem 2.8, dass H weniger als $|H|$ Elemente hat. Das kann nicht sein. Also ist H zyklisch.

Sei nun g ein Erzeuger von G und sei d ein Teiler von $|G|$. Dann hat das Element $h = g^{|G|/d}$ die Ordnung d; es erzeugt also eine Untergruppe H von G der Ordnung d.

Wir zeigen, dass es keine andere gibt. Die Untergruppe H hat nach obigem Argument genau $\varphi(d)$ Erzeuger. Diese Erzeuger haben alle die Ordnung d. Andererseits sind das auch alle Elemente der Ordnung d in G. Damit ist H die einzige zyklische Untergruppe von G der Ordnung d und da alle Untergruppen von G zyklisch sind, ist H auch die einzige Untergruppe der Ordnung d von G.

Übung 2.22
Nach Theorem 2.9 ist die Ordnung von g von der Form $\prod_{p||G|} p^{x(p)}$ mit $0 \leq x(p) \leq e(p) - f(p)$ für alle $p \mid |G|$. Nach Definition von $f(p)$ gilt aber sogar $x(p) = e(p) - f(p)$ für alle $p \mid |G|$.

Übung 2.24
Nach Korollar 2.1 ist die Abbildung wohldefiniert. Aus den Potenzgesetzen folgt, dass die Abbildung ein Homomorphismus ist. Weil g ein Erzeuger von G ist, folgt die Surjektivität. Aus Korollar 2.1 folgt schließlich die Injektivität.

Übung 2.27
2, 3, 5, 7, 11 sind Primitivwurzeln mod 3, 5, 7, 11, 13.

Übung 3.1
Der Schlüssel ist 8 und der Klartext ist BANKGEHEIMNIS.

Übung 3.3
Die Entschlüsselungsfunktion, eingeschränkt auf des Bild der Verschlüsselungsfunktion, ist deren Umkehrfunktion.

Übung 3.5
Die Konkatenation ist offensichtlich assoziativ. Das neutrale Element ist der leere String ε. Die Halbgruppe ist keine Gruppe, weil die Elemente im allgemeinen keine Inversen haben.

Übung 3.7
1. Kein Verschlüsselungssystem, weil die Abbildung nicht injektiv ist, also keine Entschlüsselungsfunktion definiert werden kann. Ein Beispiel: Sei $k = 2$. Der Buchstabe A entspricht der Zahl 0, die auf 0, also auf A, abgebildet wird. Der Buchstabe N entspricht der Zahl 13, die auf $2 * 13 \mod 26 = 0$, also auch auf A, abgebildet wird. Die Abbildung ist nicht injektiv und nach Übung 3.3 kann also kein Verschlüsselungsverfahren vorliegen.
2. Das ist ein Verschlüsselungssystem. Der Klartext- und Schlüsseltextraum ist Σ^*. Der Schlüsselraum ist $\{1, 2, \ldots, 26\}$. Ist k ein Schlüssel und $(\sigma_1, \sigma_2, \ldots, \sigma_n)$ ein Klartext, so ist $(k\sigma_1 \mod 26, \ldots, k\sigma_n \mod 26\}$ der Schlüsseltext. Das beschreibt die Verschlüsselungsfunktion zum Schlüssel k. Die Entschlüsselungsfunktion erhält man genauso. Man ersetzt nur k durch sein Inverses mod 26.

Übung 3.9
Die Anzahl der Bitpermutationen auf $\{0,1\}^n$ ist $n!$. Die Anzahl der zirkulären Links- oder Rechtsshifts auf dieser Menge ist n

Übung 3.11
Die Abbildung, die 0 auf 1 und umgekehrt abbildet, ist eine Permutation, aber keine Bitpermutation.

Übung 3.13
Gruppeneigenschaften sind leicht zu verifizieren. Wir zeigen, dass S_3 nicht kommutativ ist. Es gilt

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

aber

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\circ\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

Übung 3.15
ECB-Mode: 011100011100
CBC-Mode: 011001010000
CFB-Mode: 100010001000
OFB-Mode: 101010101010.

Übung 3.17
Definiere eine Blockchiffre mit Blocklänge n folgendermaßen: Der Schlüssel ist der Koeffizientenvektor $(c_1,\ldots,c_n)$. Ist $w_1w_2\ldots w_n$ ein Klartextwort, so ist das zugehörige Schlüsseltextwort $w_{n+1}w_{n+2}\ldots w_{2n}$ definiert durch

$$w_i=\sum_{j=1}^{n}c_jw_{i-j} \bmod 2,\quad n<i\le 2n.$$

Dies ist tatsächlich eine Blockchiffre, weil die Entschlüsselung gemäß der Formel

$$w_i=w_{n+i}+\sum_{j=1}^{n-1}c_jw_{n+i-j} \bmod 2,\quad 1\le i\le n$$

erfolgen kann. Wählt man als Initialisierungsvektor den Stromchiffreschlüssel $k_1k_2\ldots k_n$ und $r=n$, so erhält man die Stromchiffre.

Übung 3.19
Ist

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix},$$

so ist $\det A = a_{1,1}a_{2,2}a_{3,3} - a_{1,1}a_{2,3}a_{3,2} - a_{1,2}a_{2,1}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - a_{1,3}a_{2,2}a_{3,1}$.

Übung 3.21
Die Inverse ist

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Übung 3.22
Wir wählen als Schlüssel die Matrix

$$A = \begin{pmatrix} x & 0 & 0 \\ 0 & y & 0 \\ 0 & 0 & z \end{pmatrix}, \quad b = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Dann müssen die Kongruenzen

$$\begin{aligned} 17x &\equiv 6 \bmod 26 \\ 14y &\equiv 20 \bmod 26 \\ 19z &\equiv 19 \bmod 26 \end{aligned}$$

gelten. Die sind alle drei lösbar, nämlich mit $x = 8$, $y = 20$, $z = 1$. Damit ist die affin lineare Chiffre bestimmt.

Übung 4.2
Nach Definition der perfekten Sicherheit müssen wir prüfen, ob $\Pr(\vec{p}|\vec{c}) = \Pr(\vec{p})$ gilt für jeden Chiffretext $\vec{c}$ und jeden Klartext $\vec{p}$. Für $n \geq 2$ ist das falsch. Wir geben ein Gegenbeispiel. Sei $\vec{p} = (0, 0)$ und $\vec{c} = (0, 0)$. Dann ist $\Pr(\vec{p}) = 1/4$ und $\Pr(\vec{p}|\vec{c}) = 1$.

Übung 4.3
Angenommen, das Kryposystem ist perfekt geheim. Wir wenden den Satz von Bayes an und erhalten für alle Klartexte P

$$\Pr(C\,|\,P) = \frac{\Pr(P\,|\,C)\Pr(C)}{\Pr(P)} = \frac{\Pr(P)\Pr(C)}{\Pr(P)} = \Pr(C). \tag{17.3}$$

Also ist $\Pr(C\,|\,P)$ unabhängig von P.

Ist umgekehrt $\Pr(C\,|\,P)$ unabhängig von P, so gilt

$$\Pr(P\,|\,C) = \frac{\Pr(C\,|\,P)\Pr(P)}{\Pr(C)} = \frac{\Pr(C)\Pr(P)}{\Pr(C)} = \Pr(P). \tag{17.4}$$

Übung 4.4

Bei der Berechnung von C_0 wird der Zähler $\mathrm{IV} = 0^n$ verwendet und bei der Berechnung von C der Zähler $\mathrm{IV} = 0^{n-1}1$. Für $b = 0$ liefert die Verschlüsselung im CBC-CTR-Mode $C_0 = \mathbf{Enc}(K, 0^n \oplus 0^n) = \mathbf{Enc}(K, 0^n)$ und $C = \mathbf{Enc}(K, 0^n \oplus 0^{n-1}1) = \mathbf{Enc}(K, 0^{n-1}1)$. Hier sind also die beiden Chiffretexte verschieden, weil die Verschlüsselungsfunktion einer Blockchiffre injektiv ist. Für $b = 1$ liefert die Verschlüsselung $C_0 = \mathbf{Enc}(K, 0^n \oplus 0^n) = \mathbf{Enc}(K, 0)$ und $C = \mathbf{Enc}(K, 0^{n-1}1 \oplus 0^{n-1}1) = \mathbf{Enc}(K, 0^n)$. Die beiden Chiffretexte sind gleich.

Übung 5.1

Der Schlüssel ist

$$K = 0001001100110100010101110111100110011011101111001101111111110001.$$

Der Klartext ist

$$P = 0000000100100011010001010110011111000100110101011110011011110111 1.$$

Damit gilt für die Generierung der Rundenschlüssel

$$\begin{aligned}
C_0 &= 11110000110011001010101111 \\
D_0 &= 01010101011001100111100011 11 \\
v &= 1 \\
C_1 &= 11100001100110010101011111 \\
D_1 &= 10101010110011001111000111 10 \\
v &= 1 \\
C_2 &= 11000011001100101010111111 \\
D_2 &= 01010101100110011110001111 01.
\end{aligned}$$

In der ersten Runde der Feistelchiffre ist

$$\begin{aligned}
L_0 &= 11001100000000000110011001111111 \\
R_0 &= 11110000101010101111000010101010 \\
k_1 &= 000110110000001011101111111111000111000001110010 \\
E(R_0) &= 01111010000101010101010101111010000101010101010101 \\
B &= 011000010001011110111010100001100110010100100111.
\end{aligned}$$

S	1	2	3	4	5	6	7	8
Wert	5	12	8	2	11	5	9	7
C	0101	1100	1000	0010	1011	0101	1001	0111

$$\begin{aligned}
f_{k_1}(R_0) &= 00000011010010111010100110111011 \\
L_1 &= 11110000101010101111000010101010 \\
R_1 &= 11001111010010110110010101000100.
\end{aligned}$$

In der zweiten Runde der Feistelchiffre ist

$$\begin{aligned}
L_1 &= 11110000101010101111000010101010 \\
R_1 &= 11001111010010110110010101000100 \\
k_2 &= 011110011010111011011001110110111100100111100101 \\
E(R_1) &= 01100101111010100101011010110000101010100000 1001 \\
B &= 000111000100010010001111011010110110001111101100.
\end{aligned}$$

S	1	2	3	4	5	6	7	8
Wert	4	8	13	3	0	10	10	14
C	0100	1000	1101	0011	0000	1010	1010	1110

$$\begin{aligned}
f_{k_2}(R_1) &= 10111100011010101000010100100001 \\
L_2 &= 11001111010010110110010101000100 \\
R_2 &= 01001100110000000111010110001011.
\end{aligned}$$

Übung 5.3

Wir beweisen die Behauptung zuerst für jede Runde. Man verifiziert leicht, dass $E(\bar{R}) = \overline{E(R)}$ gilt, wobei E die Expansionsfunktion des DES und $R \in \{0,1\}^{32}$ ist. Ist $i \in \{1,2,\ldots,16\}$ und $K_i(k)$ der i-te DES-Rundenschlüssel für den DES-Schlüssel k, dann gilt ebenso $K_i(\bar{k}) = \overline{K_i(k)}$. Wird also k durch $\bar{k}$ ersetzt, so werden alle Rundenschlüssel K durch $\bar{K}$ ersetzt. Wird in einer Runde R durch $\bar{R}$ und K durch $\bar{K}$ ersetzt, so ist gemäß (5.3) die Eingabe für die S-Boxen $\overline{E(R)} \oplus \bar{K}$. Nun gilt $a \oplus b = \bar{a} \oplus \bar{b}$ für alle $a, b \in \{0,1\}$. Daher ist die Eingabe für die S-Boxen $E(R) \oplus K$. Da die initiale Permutation mit der Komplementbildung vertauschbar ist, gilt die Behauptung.

Übung 5.5

1.) Dies ergibt sich unmittelbar aus der Konstruktion.

2.) Sei $K_i = (K_{i,0}, \ldots, K_{i,47})$ der i-te Rundenschlüssel und sei $C_i = (C_{i,0}, \ldots, C_{i,27})$ und $D_i = (D_{i,0}, \ldots, D_{i,27})$, $1 \leq i \leq 16$.
Es gilt $K_i = \mathrm{PC2}(C_i, D_i)$. Die Funktion PC2 wählt Einträge ihrer Argumente gemäß Tab. 5.5 aus. Die zugehörige Auswahlfunktion für die Indizes sei g. Es ist also $g(1) = 14$, $g(2) = 17$ etc. Die Funktion g ist injektiv, aber nicht surjektiv, weil $9, 18, 22, 25$ keine Funktionswerte sind. Die inverse Funktion auf der Bildmenge sei g^{-1}. Sei $i \in \{0, \ldots, 26\}$. Wir unterscheiden zwei Fälle. Im ersten ist $i + 1 \notin \{9, 18, 22, 25\}$; $i + 1$ ist also ein Bild unter g. Aus der ersten Behauptung der Übung und wegen $K_1 = K_{16}$ folgt $C_{1,i} = C_{16,i+1} = K_{16,g^{-1}(i+1)} = K_{1,g^{-1}(i+1)} = C_{1,i+1}$. Im zweiten Fall ist $i + 1 \in \{9, 18, 22, 25\}$. Dann ist i ein Bild unter g und es folgt wie oben $C_{16,i} = C_{16,i+1} = K_{16,g^{-1}(i+1)} = K_{1,g^{-1}(i+1)} = C_{1,i+1}$. Damit ist gezeigt, dass $C_{1,0} = C_{1,1} = \ldots = C_{1,8}$, $C_{1,9} = \ldots = C_{1,17}$, $C_{1,18} = \ldots = C_{1,21}$, $C_{1,22} = \ldots = C_{1,24}$ und $C_{1,25} = \ldots = C_{1,27}$. Man zeigt $C_{1,8} = C_{1,9}$, $C_{1,17} = C_{1,18}$, $C_{1,21} = C_{1,22}$ und $C_{1,24} = C_{1,25}$ analog, aber unter Verwendung von $K_1 = K_2$. Entsprechend beweist man die Behauptung für D_i.

3.) Man kann entweder alle Bits von C_1 auf 1 oder 0 setzen und für D_1 genauso. Das gibt vier Möglichkeiten.

Übung 5.6

Alle sind linear bis auf die S-Boxen. Wir geben ein Gegenbeispiel für die erste S-Box. Es ist $S_1(000000) = 1110$, $S_1(111111) = 1101$, aber $S_1(000000) \oplus S_1(111111) = 1110 \oplus 1101 = 0011 \neq 1101 = S_1(111111) = S_1(000000 \oplus 111111)$.

Übung 6.2

`InvShiftRows`: Zyklischer Rechtsshift um c_i Positionen mit den Werten c_i aus Tab. 6.1.

`InvSubBytes`: $b \mapsto (A_{-1}(b \oplus c))^{-1}$. Diese Funktion ist in Tab. 17.1 dargestellt. Diese Tabelle ist folgendermaßen zu lesen. Um den Funktionswert von $\{uv\}$ zu finden, sucht man das Byte in Zeile u und Spalte v, So ist zum Beispiel `InvSubBytes({a5}) = {46}`.

`InvMixColumns`: Das ist die lineare Transformation

$$s_j \leftarrow \begin{pmatrix} \{0e\} & \{0b\} & \{0d\} & \{09\} \\ \{09\} & \{0e\} & \{0b\} & \{0d\} \\ \{0d\} & \{09\} & \{0e\} & \{0b\} \\ \{0b\} & \{0d\} & \{09\} & \{0e\} \end{pmatrix} s_j, \quad 0 \leq j < \mathrm{Nb}.$$

Übung 7.1

Es ist $2^{1110} \equiv 1024 \bmod 1111$.

Tab. 17.1 `InvSubBytes`

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Übung 7.3
Die kleinste Pseudoprimzahl zur Basis 2 ist 341. Es ist $341 = 11 * 31$ und $2^{340} \equiv 1 \bmod 341 = 1$.

Übung 7.5
Sei n eine Charmichael-Zahl. Nach Definition ist sie keine Primzahl und nach Theorem 7.4 ist sie quadratfrei, also keine Primzahlpotenz. Also hat n wenigstens zwei Primteiler. Sei $n = pq$ mit Primfaktoren p, q, $p > q$. Nach Theorem 7.5 ist $p - 1$ ein Teiler von $n - 1 = pq - 1 = (p - 1)q + q - 1$. Daraus folgt, dass $p - 1$ ein Teiler von $q - 1$ ist. Aber das ist unmöglich, weil $0 < q - 1 < p - 1$ ist. Damit ist die Behauptung bewiesen.

Übung 7.7
Wir beweisen, dass 341 zusammengesetzt ist. Dazu schreiben wir $340 = 4 * 85$. Es ist $2^{85} \equiv 32 \bmod 341$ und $2^{170} \equiv 1 \bmod 341$. Also ist n zusammengesetzt.

Übung 7.9
Die kleinste 512-Bit-Primzahl ist $2^{512} + 3$.

Übung 8.1
Ist $de - 1$ ein Vielfaches von $p - 1$ und von $q - 1$, so zeigt man wie im Beweis von Theorem 8.1, dass $m^{ed} \equiv m \bmod p$ und $m^{ed} \equiv m \bmod q$ für jedes $m \in \{0, 1, \ldots, n - 1\}$ gilt, woraus nach dem chinesischen Restsatz $m^{ed} \equiv m \bmod n$ folgt.

Übung 8.3
Setze $p = 223$, $q = 233$, $n = 51959$, $e = 5$. Dann ist $d = 10301$, $m = 27063$, $c = 50042$.

Übung 8.5
Wir skizzieren einen einfachen Intervallschachtelungsalgorithmus. Setze $m_0 = 1$, $m_1 = c$. Dann wiederhole folgende Berechnungen, bis $m_1^e = c$ oder $m_0 = m_1$ ist: Setze $x = \lfloor (m_1 - m_0)/2 \rfloor$. Wenn $x^e \geq c$ ist, dann setze $m_1 = x$. Sonst setze $m_0 = x$. Ist nach der letzten Iteration $m_1^e = c$, so ist die e-te Wurzel von c gefunden. Andernfalls existiert sie nicht.

Übung 8.7
Es werden 16 Quadrierungen und eine Multiplikation benötigt.

Übung 8.9
Man berechnet die Darstellung $1 = xe + yf$ und dann $c_e^x c_f^y = m^{xe+yf} = m$.

Übung 8.11
Es ist $p = 37$, $q = 43$, $e = 5$, $d = 605$, $y_p = 7$, $y_q = -6$, $m_p = 9$, $m_q = 8$, $m = 1341$.

Übung 8.13
Da e teilerfremd zu $(p-1)(q-1)$ ist, gilt für die Ordnung k der primen Restklasse $e + \mathbb{Z}(p-1)(q-1)$: $e^k \equiv 1 \bmod (p-1)(q-1)$. Daraus folgt $c^{e^{k-1}} \equiv m^{e^k} \equiv m \bmod n$. Solange k groß ist, stellt dies keine Bedrohung dar.

Übung 8.15
Ja, denn die Zahlen $(x_5 2^5 + x_4 2^4 + x_3 2^3 + x_2 2^2) \bmod 253$, $x_i \in \{0, 1\}$, $2 \leq i \leq 5$, sind paarweise verschieden.

Übung 8.17
Low-Exponent-Attack: Wenn eine Nachricht $m \in \{0, 1, \ldots, n-1\}$ mit dem Rabin-Verfahren unter Verwendung der teilerfremden Moduln n_1 und n_2 verschlüsselt wird, entstehen die Schlüsseltexte $c_i = m^2 \bmod n_i$, $i = 1, 2$. Der Angreifer bestimmt eine Zahl $c \in \{0, \ldots, n_1 n_2 - 1\}$ mit $c \equiv c_i \bmod n_i$, $i = 1, 2$. Dann ist $c = m^2$, und m kann bestimmt werden, indem aus c die Quadratwurzel gezogen wird. Gegenmaßnahme: Randomisierung einiger Nachrichtenbits.

Multiplikativität: Wenn Bob die Schlüsseltexte $c_i = m_i^2 \bmod n$, $i = 1, 2$, kennt, dann kann er daraus den Schlüsseltext $c_1 c_2 \bmod n = (m_1 m_2)^2 \bmod n$ berechnen. Gegenmaßnahme: spezielle Struktur der Klartexte.

Übung 8.19
Wenn $(B_1 = g^{b_1}, C_1 = A^{b_1} m_1)$, $(B_2 = g^{b_2}, C_2 = A^{b_2} m_2)$ die Schlüsseltexte sind, dann ist auch $(B_1 B_2, C_1 C_2 = A^{b_1+b_2} m_1 m_2)$ ein gültiger Schlüsseltext. Er verschlüsselt $m_1 m_2$. Man kann diese Attacke verhindern, wenn man nur Klartexte von spezieller Gestalt erlaubt.

Übung 8.21
Der Klartext ist $m = 37$.

Übung 9.1
Da $x^2 \geq n$ ist, ist $\lceil \sqrt{n} \rceil = 115$ der kleinstmögliche Wert für x. Für dieses x müssen wir prüfen, ob $z = n - x^2$ ein Quadrat ist. Wenn nicht, untersuchen wir $x + 1$. Es ist $(x+1)^2 = x^2 + 2x + 1$. Daher können wir $(x+1)^2$ berechnen, indem wir zu x^2 den Wert $2x + 1$ addieren. Wir finden schließlich, dass $13199 = 132^2 - 65^2 = (132 - 65)(132 + 65) = 67 * 197$ ist. Nicht jede zusammengesetzte natürliche Zahl ist Differenz von zwei Quadraten. Daher funktioniert das Verfahren nicht immer. Wenn es funktioniert, braucht es $O(\sqrt{n})$ Operationen in $\mathbb{Z}$.

Übung 9.3
Die Faktorisierung $n = 11617 * 11903$ findet man, weil $p - 1 = 2^5 * 3 * 11^2$ und $q = 2 * 11 * 541$ ist. Man kann also $B = 121$ setzen.

Übung 9.5
Die Anzahl der Primzahlen $\leq B$ ist $O(B/\log B)$ nach Theorem 7.2. Jede der Primzahlpotenzen, deren Produkt k bildet, ist $\leq B$. Damit ist $k = O(B^{B/\log B}) = O(2^B)$. Die Exponentiation von a mit k mod n erfordert nach Theorem 2.15 $O(B)$ Multiplikationen mod n.

Übung 9.7
Es ist $m = 105$. Man erhält mit dem Siebintervall $-10, \ldots, 10$ und der Faktorbasis $\{-1, 2, 3, 5, 7, 11, 13\}$ die zerlegbaren Funktionswerte $f(-4) = -2 * 5 * 7 * 13$, $f(1) = 5^3$, $f(2) = 2 * 13^2$, $f(4) = 2 * 5 * 7 * 11$, $f(6) = 2 * 5 * 11^2$. Man erhält daraus die Kongruenz $(106 * 107 * 111)^2 \equiv (2 * 5^2 * 11 * 13)^2 \bmod n$. Also ist $x = 106 * 107 * 111$, $y = 2 * 5^2 * 11 * 13$ und damit $\gcd(x - y, n) = 41$.

Übung 10.1
Der DL ist $x = 323$.

Übung 10.3
Die kleinste Primitivwurzel mod 1117 ist 2. Der DL ist $x = 96$.

Übung 10.5
Die kleinste Primitivwurzel mod 3167 ist 5 und es gilt $5^{1937} \equiv 15 \bmod 3167$.

Übung 10.7
Die kleinste Primitivwurzel mod $p = 2039$ ist $g = 7$. Es gilt $7^{1344} \equiv 2 \bmod p$, $7^{1278} \equiv 3 \bmod p$, $7^{664} \equiv 5 \bmod p$, $7^{861} \equiv 11 \bmod p$, $7^{995} \equiv 13 \bmod p$.

Übung 11.1
Sei n ein 1024-Bit Rabin-Modul (siehe Abschn. 8.4). Die Funktion $\mathbb{Z}_n \to \mathbb{Z}_n$, $x \mapsto x^2 \bmod n$ ist eine Einwegfunktion, falls n nicht faktorisiert werden kann. Das folgt aus den Überlegungen in Abschn. 8.4.5.

Übung 11.3
Der maximale Wert von $h(k)$ ist 9999. Daraus ergibt sich die maximale Länge der Bilder zu 14. Eine Kollision ist $h(1) = h(10948)$.

Übung 12.1
Es ist $n = 127 * 227$, $e = 5$, $d = 22781$, $s = 5876$.

Übung 12.3
Die Signatur ist eine Quadratwurzel mod n aus dem Hashwert des Dokuments. Die Hashfunktion muss aber so ausgelegt werden, dass ihre Werte nur Quadrate mod n sind. Die Sicherheits- und Effizienzüberlegungen entsprechen denen in Abschn. 8.4.

Übung 12.5
Es ist $A^r r^s = A^q (q^{(p-3)/2})^{h(m)-qz}$. Weil $gq \equiv -1 \bmod p$ ist, gilt $q \equiv -g^{-1} \bmod p$. Außerdem ist $g^{(p-1)/2} \equiv -1 \bmod p$, weil g eine Primitivwurzel mod p ist. Daher ist $q^{(p-3)/2} \equiv (-g)^{(p-1)/2} g \equiv g \bmod p$. Insgesamt hat man also $A^r r^s \equiv A^q g^{h(m)} g^{-qz} \equiv A^q g^{h(m)} A^{-q} \equiv g^{h(m)} \bmod p$. Die Attacke funktioniert, weil g ein Teiler von $p-1$ ist und der DL z von A^q zur Basis g^q berechnet werden konnte. Man muss das also verhindern.

Übung 12.7
Es ist $r = 799$, $k^{-1} = 1979$, $s = 1235$.

Übung 12.9
Es ist $q = 43$. Der Erzeuger der Untergruppe der Ordnung q ist $g = 1984$. Weiter ist $A = 834$, $r = 4$, $k^{-1} = 31$ und $s = 23$.

Übung 12.11
Sie lautet $g^s = A^r r^{h(x)}$.

Übung 13.1
Wir müssen dazu ein irreduzibles Polynom vom Grad 2 über GF(3) konstruieren. Das Polynom $x^2 + 1$ ist irreduzibel über GF(3), weil es keine Nullstelle hat. Der Restklassenring mod $f(X) = X^2 + 1$ ist also GF(9). Bezeichne mit α die Restklasse von X mod $f(X)$. Dann gilt also $\alpha^2 + 1 = 0$. Die Elemente von GF(9) sind 0, 1, 2, α, 2α, $1 + \alpha$, $1 + 2\alpha$, $2 + \alpha$, $2 + 2\alpha$. Die Additionstabelle ergibt sich unter Verwendung der Rechenregeln in $\mathbb{Z}/3\mathbb{Z}$. Für die Multiplikationstabelle braucht man zusätzlich die Regel $\alpha^2 = -1$.

Übung 13.3
Die Punkte sind $\mathcal{O}$, $(0, 1)$, $(0, 6)$, $(2, 2)$, $(2, 5)$. Die Gruppe hat also die Ordnung 5 und ist damit zyklisch. Jeder Punkt $\neq \mathcal{O}$ ist ein Erzeuger.

Übung 14.1
Alice wählt zufällig und gleichverteilt einen Exponenten $b \in \{0, 1, \ldots, p-2\}$ und berechnet $B = g^b \bmod p$. Sie schickt B an Bob. Bob wählt $e \in \{0, 1\}$ zufällig und gleichverteilt und schickt e an Alice. Alice schickt $y = (b + ea) \bmod (p - 1)$ an Bob. Bob verifiziert $g^y \equiv A^e B \bmod p$. Das Protokoll ist vollständig, weil jeder, der den geheimen Schlüssel von Alice kennt, sich erfolgreich identifizieren kann. Wenn Alice das richtige y für $e = 0$ und für $e = 1$ zurückgeben kann, kennt sie den DL a. Daher kann sie nur mit Wahrscheinlichkeit $1/2$ betrügen. Das Protokoll ist also korrekt. Das Protokoll kann von Bob simuliert werden. Er wählt gleichverteilt zufällig $y \in \{0, 1, \ldots, p - 2\}$, $e \in \{0, 1\}$ und setzt $B = g^y A^{-e} \bmod p$. Damit funktioniert das Protokoll und die Wahrscheinlichkeitsverteilungen sind dieselben wie im Originalprotokoll.

Übung 14.3
Ein Betrüger muss Zahlen x und y liefern, die das Protokoll erfüllen. Wenn er x mitteilt, kennt er das zufällige $e = (e_1, \ldots, e_k)$ nicht. Wäre er in der Lage, nach Kenntnis von e noch ein korrektes y zu produzieren, könnte er Quadratwurzeln mod n berechnen. Das kann er aber nicht. Also kann er x nur so so wählen, dass er die richtige Antwort y für genau einen Vektor $e \in \{0, 1\}^k$ geben kann. Er kann sich also nur mit Wahrscheinlichkeit 2^{-k} richtig identifizieren.

Übung 14.5
Der Signierer wählt r zufällig, berechnet $x = r^2 \bmod n$, $(e_1, \ldots, e_k) = h(x \circ m)$ und $y = r \prod_{i=1}^{k} s_i^{e_i}$. Die Signatur ist (x, y).

Übung 15.2
Es gilt $a(X) = a_1 X + s = 2x + 3$, $y_1 = 5$, $y_2 = 7$, $y_3 = 9$, $y_4 = 0$.