Aufgabe 3.9

(a) $\mathbb{Z}_8^*$?

×	**1**	**3**	**5**	**7**
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

(b) Nein, denn wegen $a^2 = 1$ für alle $a \in \mathbb{Z}_8^*$ kann kein Element die gesamte Gruppe (multiplikativ) erzeugen.

Aufgabe 3.10

(a) $\mathbb{Z}_5^*$

×	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(b) erzeugende Elemente: 2 und 3

Aufgabe 3.11

Ist p eine Primzahl, so gibt es $\varphi(p-1)$ erzeugende Elemente in $\mathbb{Z}_p^*$.

(a) Für $p = 11$ gilt $\varphi(11-1) = \varphi(10) = 4$
Somit müssen es 4 erzeugende Elemente sein.

(b) $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$, ...
Also ist $a = 2$ erzeugend, d. h. eine Primitivwurzel.

Aufgabe 3.12

Die Rechenregeln lauten

- $\varphi(p) = p - 1$, wenn p eine Primzahl ist.
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ wenn $\text{ggt}(a, b) = 1$
- $\varphi(p^n) = \varphi(a) \cdot p^{n-1}$, wenn p eine Primzahl ist.

(a) $\varphi(47) = 46$ (47 ist prim)

(b) $\varphi(2^4) = \varphi(2) \cdot 2^3 = 1 \cdot 8 = 8$

(c) $\varphi(27) = \varphi(3) \cdot 3^2 = 18$

(d) $\varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$

(e) $\varphi(77) = \varphi(7 \cdot 11) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$

(f) $\varphi(50) = \varphi(2 \cdot 5^2) = \varphi(2) \cdot \varphi(5) \cdot 5 = 1 \cdot 4 \cdot 5 = 20$

(g) $\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = \varphi(2) \cdot 2^2 \cdot \varphi(3) \cdot \varphi(5) = 1 \cdot 4 \cdot 2 \cdot 4 = 32$

(h) $\varphi(10000) = \varphi(2^4 \cdot 5^4) = \varphi(2) \cdot 2^3 \cdot \varphi(5) \cdot 5^3 = 8 \cdot 4 \cdot 125 = 4000$

Aufgabe 3.13

(a)

$10 = 2 \cdot 5$	$14^2 = 6$
$5 = 2 \cdot 2 + 1$	$13 \cdot 17^2 = 14$
$2 = 2 \cdot 1$	$13^2 = 17$
$1 = 2 \cdot 0 + 1$	$13 \cdot 1^2 = 13$

(b)

$16 = 2 \cdot 8$	$6^2 = 17$
$8 = 2 \cdot 4$	$5^2 = 6$
$4 = 2 \cdot 2$	$9^2 = 5$
$2 = 2 \cdot 1$	$3^2 = 9$
$1 = 2 \cdot 0 + 1$	$3 \cdot 1^2 = 3$

Aufgabe 3.14

$\frac{41 \cdot 40}{2} = 41 \cdot 20 = 820$ Schlüssel

Aufgabe 3.15

Beim DHM-Schlüsselaustauch geht es darum, wie Alice und Bob über einen nicht abhörsicheren Kanal einen geheimen Schlüssel in Form einer Zahl vereinbaren können.

Aufgabe 3.16

1. Alice und Bob einigen sich (öffentlich) auf eine grosse Primzahl p und eine Primitivwurzel g modulo p.
2. Alice wählt ihren (geheimen) Exponenten $a = 4$, berechnet damit die Zahl $A = g^a \mod p = 2^4 \mod 13 = 3$ und sendet sie an Bob.
3. Bob wählt seinen (geheimen) Exponenten $b = 5$, berechnet damit die Zahl $B = g^b \mod p = 2^5 \mod 13 = 6$ und sendet diese Zahl an Alice.
4. Alice berechnet $B^a \mod p = 6^4 \mod 13 = 9$
5. Bob berechnet $A^b \mod p = 3^5 \mod 13 = 9$

Die Potenzen können effizient mit dem Square-and-Multiply-Algorithmus berechnet werden. Die Exponenten a und b müssen geheim bleiben.

Aufgabe 3.17

Obwohl die Zahlen p, g und die ausgerechnete Potenzen $g^a = A$ und $g^b = B$ durch Abhören in Erfahrung gebracht werden können, lassen sich damit (nach heutigem Wissensstand) die geheimen Exponenten a und b von Alice bzw. Bob nicht effizient („innert nützlicher Zeit“) berechnen. Voraussetzung ist aber, dass die Primzahl p sehr gross ist.

Die Aufgabe, $a = \log_g A$ bzw. $b = \log_g B$ modulo p zu bestimmen, wird auch das *Diskrete-Logarithmus-Problem (DLP)* genannt. Mit *diskret* ist hier ganzzahlig gemeint.

Aufgabe 3.18

(a) Es handelt sich um den *Man-in-the-Middle*-Angriff. Dabei leitet Eve die Kommunikation zwischen Alice und Bob über sich um und gibt sich gegenüber Bob als Alice und gegenüber Alice als Bob aus. Dabei führt sie mit beiden einen eigenen Schlüsselaustausch durch und kann so die verschlüsselte Kommunikation abhören oder eigene Nachrichten einfliessen lassen.

(b) Alice und Bob müssen die ausgetauschten Nachrichten in irgend einer Form authentifzieren können. Zum Beispiel durch eine digitale Signatur.

Aufgabe 3.19

Es handelt sich um ein kryptographisches Verfahren, bei dem zum Verschlüsseln ein öffentlicher Schlüssel (e) und zum Entschlüsseln ein privater Schlüssel (d) verwendet wird.

Das Schlüsselpaar hat die folgenden Eigenschaften:

- Der geheime Schlüssel (d) lässt sich nicht aus dem öffentlichen Schlüssel e berechnen. (Deshalb wird das Verfahren auch *asymmetrisch* genannt.)
- Für jede Nachricht m gilt: $D_d(E_e(m)) = m$
- Für jede Nachricht m gilt: $E_e(D_d(m)) = m$ (Signatur-Eigenschaft)

Aufgabe 3.20

Sie baut darauf auf, dass es bis zum heutigen Tag kein effizientens Verfahren zur Faktorisierung eines Produkts aus zwei grossen Primzahlen gibt.

Aufgabe 3.21

(a)

a	b
258	45
45	33
33	12
12	9
9	3
3	0

$\mathrm{ggT}(258, 45) = 3$

(b)

a	b
392	135
135	122
122	13
13	5
5	3
3	2
2	1
1	0

$\text{ggT}(392, 135) = 1$

Aufgabe 3.22

(a)

a	b	$\lfloor a/b \rfloor$	x	y
36	15	2	-2	5
15	6	2	1	-2
6	3	2	0	1
3	0	-	1	0

$\text{ggT}(36, 15) = 3 = -2 \cdot 36 + 5 \cdot 15$

(b)

a	b	$\lfloor a/b \rfloor$	x	y
47	20	2	3	-7
20	7	2	-1	3
7	6	1	1	-1
6	1	6	0	1
1	0	-	1	0

$\text{ggT}(47, 20) = 1 = 3 \cdot 47 - 7 \cdot 20$

Aufgabe 3.23

(a)

p	a	$\lfloor p/a \rfloor$	x	y
7	3	2	1	-2
3	1	3	0	1
1	0	-	1	0

also ist $1 = 1 \cdot 7 + (-2) \cdot 3$

Rechnet man die Gleichung modulo 7, so entfällt der Summand $1 \cdot 7$ und es bleibt:

$1 \pmod 7 = -2 \cdot 3 \pmod 7 = 5 \cdot 3 \pmod 7$.

Also ist 5 die multiplikative Inverse von 3 in $\mathbb{Z}_7^*$.

(b)

a	b	$\lfloor a/b \rfloor$	x	y
19	11	1	-4	7
11	8	1	3	-4
8	3	2	-1	3
3	2	1	1	-1
2	1	2	0	1
1	0	-	1	0

$1 = (-4) \cdot 19 + 7 \cdot 11$

Rechnet man die Gleichung modulo 19, so verschwindet der erste Summand:

$1 \pmod{19} = 7 \cdot 11 \pmod{19}$

Also ist 7 die multiplikative Inverse von 11 in $\mathbb{Z}_{19}^*$.

Aufgabe 3.24

(a) Für zwei teilerfremde Zahlen a und n gilt: $a^{\varphi(n)} \equiv 1 \mod n$

(b) $a = 5$, $n = 6$: $5^{\varphi(6)} \mod 6 \equiv 5^2 \mod 6 \equiv 25 \mod 6 \equiv 1 \mod 6$

Aufgabe 3.25

(a) $E_e(m) = m^3 \equiv 2^3 \equiv 8 \mod 33$

(b) Square-and-Multiply:

$7 = 2 \cdot 3 + 1 \qquad 10 \cdot 10^2 = 10$
$3 = 2 \cdot 1 + 1 \qquad 10 \cdot 10^2 = 10$
$1 = 2 \cdot 0 + 1 \qquad 10 \cdot 1^2 = 10$

$10^7 \equiv \cdots \equiv 10 \pmod{33}$

(c) Signieren heisst, dass die Nachricht mit dem geheimen Schlüssel verschlüsselt wird:

$7 = 2 \cdot 3 + 1 \qquad 5 \cdot 26^2 = 14$
$3 = 2 \cdot 1 + 1 \qquad 5 \cdot 5^2 = 26$
$1 = 2 \cdot 0 + 1 \qquad 5 \cdot 1^2 = 5$

$5^7 \equiv= \cdots \equiv 14 \pmod{33}$

Aufgabe 3.26

1. $n = 5 \cdot 11 = 55$ (Modulus zum Ver- und Entschlüsseln)
2. $\varphi(n) = \varphi(55) = (5-1) \cdot (10-1) = 4 \cdot 10 = 40$
3. Der öffentliche Schlüssel e muss teilerfremd zu $\varphi(n) = 40$ sein. Die Zahl $e = 7$ erfüllt diese Eigenschaft.

4. Der gesuchte private Schlüssel d ist die multiplikative Inverse zu e modulo $\varphi(n)$. Erweiterter euklischen Algorithmus:

$\varphi(n)$	e	$\lfloor\varphi(n)/e\rfloor$	x	y
40	7	5	3	-17
7	5	1	-2	3
5	2	2	1	-2
2	1	2	0	1
1	0	-	1	0

   Also ist $-17 \pmod{40} = 23 \pmod{40}$ die multiplikative Inverse von 7 und damit $d = 23$ der private Schlüssel.

Man kann jetzt (fakultativ) mit einem geeigneten Programm prüfen, ob die Schlüssel tatsächlich das Gewünschte leisten:

- Wähle irgend eine Zahl $1 < m < n$: $m = 4$ (m wie *message*)
- Verschlüsseln: $c = m^e \mod n = 4^7 \mod 55 = 49$ (c wie *ciphertext*)
- Entschlüsseln: $c^d \mod n = 49^{23} \mod 5 = 4 = m$ (stimmt)

Aufgabe 3.27

1. $n = 11 \cdot 17 = 187$ (Modulus zum Ver- und Entschlüsseln)
2. $\varphi(n) = \varphi(187) = (11-1) \cdot (17-1) = 10 \cdot 16 = 160$
3. Der öffentliche Schlüssel e muss teilerfremd zu $\varphi(n)$ sein. Die Zahl $e = 3$ erfüllt diese Eigenschaft.
4. Der gesuchte private Schlüssel d ist die multiplikative Inverse zu e modulo $\varphi(n)$. Erweiterter euklischer Algorithmus:

$\varphi(n)$	e	$\lfloor\varphi(n)/e\rfloor$	x	$y = d$
160	3	53	1	-53
3	1	3	0	1
1	0	-	1	0

   Also ist $-53 \pmod{160} = 107 \pmod{160}$ die multiplikative Inverse von 3 und damit $d = 107$ der private Schlüssel.

Man kann jetzt (fakultativ) mit einem geeigneten Programm prüfen, ob die Schlüssel tatsächlich das Gewünschte leisten:

- Wähle irgend eine Zahl $1 < m < n$: $m = 23$ (m wie *message*)
- Verschlüsseln: $c = m^e \mod n = 23^3 \mod 187 = 12$ (c wie *ciphertext*)
- Entschlüsseln: $c^d \mod n = 12^{107} \mod 187 = 23 = m$ (stimmt)