Aufgabe 1.1

- *Vertraulichkeit:* Nur berechtigte Personen sollen eine Nachricht lesen können.
- *Authentifizierung:* Der Urheber einer Nachricht soll eindeutig identifizierbar sein.
- *Integrität:* Eine Nachricht soll unverändert sein.
- *Verbindlichkeit:* Der Empfänger kann nicht abstreiten, dass er vom Sender eine Nachricht mit identischem Inhalt erhalten hat.

Aufgabe 1.2

$4 \cdot 4 \cdot \ldots \cdot 4 = 4^{100}$ Nachrichten

Aufgabe 1.3

Die Sicherheit eines kryptografischen Verfahrens sollte nur auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verfahrens beruhen.

Aufgabe 1.4

(a) Ein Angreifer kann beliebigen Klartext verschlüsseln: *Chosen-plaintext attack*

(b) Einem Angreifer ist bekannt, dass `GUTENTAG` zu `XMPTFTSU` verschlüsselt wird. *Known-plaintext attack*

(c) Ein Angreifer kann beliebigen Geheimtext entschlüsseln. *Chosen-ciphertext attack*

Aufgabe 2.1

Schlüssel: Verschiebung um vier Zeichen

Klartext: `DAS WETTER IST SCHOEN`

Aufgabe 2.2

```
 GEHEIM
 EFIEFI
-------
 KJPINU
```

Aufgabe 2.3

m = `DAS ALSO IST DES PUDELS KERN`

Aufgabe 2.4

(a) Man sucht Paare, Tripel, Quadrupel gleicher Geheimtextfolgen.

(b) Man bestimmt die Abstände dieser Folgen.

(c) Der ggT dieser Abstände ist ein Kandidat für die Schlüssellänge n.

(d) Die Geheimtextzeichen, die sich jeweils im Abstand von n Zeichen befinden, sind mit dem gleichen Schlüsselbuchstaben verschlüsselt worden und können wie eine Verschiebechiffre durch eine Häufigkeitsanalyse oder durch Ausprobieren entschlüsselt werden.

Aufgabe 2.5

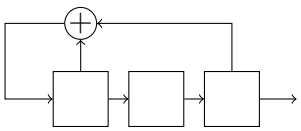
Die folgenden Zählungen beginnen bei 1:

Zeichenfolge	Positionen	Distanz(en)
`STQP`	39, 70	31
`KVNO`	72, 107	35
`YXKZ`	154, 182	28
`MQSY`	227, 290	63

Vermutlich ist die Wiederholung von `STQP` zufällig entstanden. Denn mit den übrigen Distanzen erhält man

$\mathrm{ggT}(35, 28, 63) = 7$

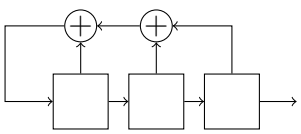
Aufgabe 2.6



Registerinhalte:	1	0	0
	1	1	0
	1	1	1
	0	1	1
	1	0	1
	0	1	0
	0	0	1
	1	0	0

Outputfolge: 0 0 1 1 1 0 1

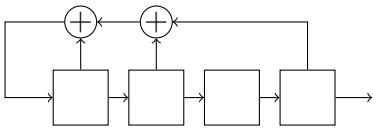
Aufgabe 2.7



Registerinhalte:	1	1	1
	1	1	1

Outputfolge: 1

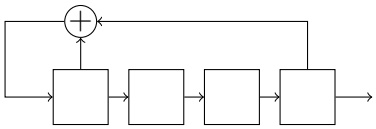
Aufgabe 2.8



Registerinhalte:				
	0	1	1	0
	1	0	1	1
	0	1	0	1
	0	0	1	0
	0	0	0	1
	1	0	0	0
	1	1	0	0
	0	1	1	0

Outputfolge: 0 1 1 0 1 0 0

Aufgabe 2.9



Registerinhalte:				
	1	0	1	1
	0	1	0	1
	1	0	1	0
	1	1	0	1
	0	1	1	0
	0	0	1	1
	1	0	0	1
	0	1	0	0
	0	0	1	0
	0	0	0	1
	1	0	0	0
	1	1	0	0
	1	1	1	0
	1	1	1	1
	0	1	1	1
	1	0	1	1

Outputfolge: 1 1 0 1 0 1 1 0 0 1 0 0 0 1 1

Aufgabe 3.1

(a) $(\mathbb{N}_0, +)$ keine Gruppe (Inverse fehlen)

(b) $(\mathbb{N}, \cdot)$ keine Gruppe (Inverse fehlen)

(c) $(\mathbb{Z}, +)$ Gruppe

(d) $(\mathbb{Z} \setminus \{0\}, \cdot)$ keine Gruppe (Inverse fehlen)

(e) $(\mathbb{Q}, +)$ Gruppe

(f) $(\mathbb{Q} \setminus \{0\}, \cdot)$ Gruppe

(g) $(\mathbb{R}, +)$ Gruppe

(h) $(\mathbb{R} \setminus \{0\}, \cdot)$ Gruppe

Aufgabe 3.2

(a) wahr, denn 5 teilt $28 - 3 = 25$

(b) wahr, denn 5 teilt $3 - 28 = -25$

(c) falsch, denn 5 teilt $28 - (-3) = 31$ nicht

(d) falsch, denn 5 teilt $-28 - 3 = -31$ nicht

(e) wahr, denn 5 teilt $-28 - (-3) = -25$

(f) wahr, denn 5 teilt $-3 - (-28) = 25$

Aufgabe 3.3

(a) $(\mathbb{Z}_6, +)$:

$+$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(b) Ja, denn alle Eigenschaften sind erfüllt

- Abgeschlossenheit: ja
- Assoziativität: ja
- Neutralelement: 0
- inverse Elemente: vollständig vorhanden

Aufgabe 3.4

(a) $(\mathbb{Z}_6 \setminus \{0\}, \times)$:

$\times$	**1**	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

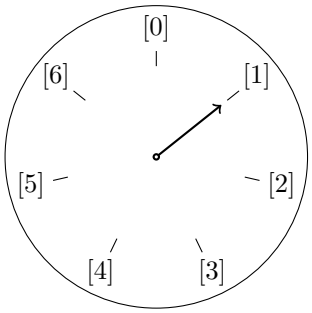
(b) Nein, denn nicht alle Eigenschaften sind erfüllt

- Abgeschlossenheit: ok
- Assoziativität: ok
- Neutralelement: 1
- inverse Elemente: unvollständig

Aufgabe 3.5

$\times$	**1**	**3**	**5**	**7**
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Aufgabe 3.6



(a) $5 + 6 = 4$

(b) $1 - 3 = 5$

(c) $3 \cdot 5 = 1$

(d) $1 : 4 = 1 \cdot 4^{-1} = 1 \cdot 2 = 2$

(e) $2 : 5 = 2 \cdot 5^{-1} = 2 \cdot 3 = 6$

Aufgabe 3.7

- $2^1 = 2$, $2^2 = 4$, $2^3 = 1$ (nicht erzeugend)
- $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$ (erzeugend)
- $4^1 = 4$, $4^2 = 2$, $4^3 = 1$ (nicht erzeugend)
- $5^1 = 5$, $5^2 = 4$, $5^3 = 6$, $5^4 = 2$, $5^5 = 3$, $5^6 = 1$ (erzeugend)
- $6^1 = 6$, $6^2 = 1$ (nicht erzeugend)

Aufgabe 3.8

(a) $1^{75} = 1$

(b) $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 6$, $2^5 = 2$, $\ldots$, $2^{59} = 8$

(c) $3^1 = 3$, $3^2 = 9$, $3^3 = 7$, $3^4 = 1$, $3^5 = 3$, $\ldots$, $3^{100} = 1$

(d) $4^1 = 4$, $4^2 = 6$, $4^3 = 4$, $\ldots$, $4^{99} = 4$

(e) $5^1 = 5$, $5^2 = 5$, $\ldots$, $5^{62} = 5$

(f) $6^1 = 6$, $6^2 = 6$, $\ldots$, $6^{111} = 6$

(g) $7^1 = 7$, $7^2 = 9$, $7^3 = 3$, $7^4 = 1$, $7^5 = 7$, $\ldots$, $7^{82} = 9$

(h) $8^1 = 8$, $8^2 = 4$, $8^3 = 2$, $8^4 = 6$, $8^5 = 8$, $\ldots$, $8^{39} = 2$

(i) $9^1 = 9$, $9^2 = 1$, $9^3 = 9$, $\ldots$, $9^{201} = 9$

Aufgabe 3.9

$73 = 2 \cdot 36 + 1$	$2 \cdot 16^2 = 2$
$36 = 2 \cdot 18$	$2^2 = 16$
$18 = 2 \cdot 9$	$2^2 = 4$
$9 = 2 \cdot 4 + 1$	$2 \cdot 16^2 = 2$
$4 = 2 \cdot 2$	$2^2 = 16$
$2 = 2 \cdot 1$	$2^2 = 4$
$1 = 2 \cdot 0 + 1$	$2 \cdot 1^2 = 2$

Aufgabe 3.10

$78 = 2 \cdot 39$	$14^2 = 2$
$39 = 2 \cdot 19 + 1$	$14 \cdot 7^2 = 6$
$19 = 2 \cdot 9 + 1$	$14 \cdot 3^2 = 7$
$9 = 2 \cdot 4 + 1$	$14 \cdot 13^2 = 3$
$4 = 2 \cdot 2$	$14^2 = 13$
$2 = 2 \cdot 1$	$14^2 = 9$
$1 = 2 \cdot 0 + 1$	$14 \cdot 1^2 = 14$

Aufgabe 3.11

(a) $\varphi(2) = 1$ (c) $\varphi(5) = 4$ (e) $\varphi(11) = 10$

(b) $\varphi(3) = 2$ (d) $\varphi(7) = 6$ (f) $\varphi(p) = p - 1$

Aufgabe 3.12

(a) $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(6) = 2$

(b) $\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(15) = 8$

(c) $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(20) = 8$

(d) $\varphi(2) = 1$, $\varphi(7) = 6$, $\varphi(14) = 6$

Aufgabe 3.13

(a) $\varphi(4) = 2$ (e) $\varphi(9) = 6$

(b) $\varphi(8) = 4$ (f) $\varphi(27) = 18$

(c) $\varphi(16) = 8$ (g) $\varphi(81) = 54$

(d) $\varphi(32) = 16$ (h) $\varphi(p^k) = p^{k-1}(p-1)$

Aufgabe 3.14

(a) $\varphi(24) = \varphi(2^3 \cdot 3) = 2^2(2-1) \cdot (3-1) = 8$

(b) $\varphi(36) = \varphi(2^2 \cdot 3^2) = 2(2-1) \cdot 3(3-1) = 12$

(c) $\varphi(100) = \varphi(2^2 \cdot 5^2) = 2(2-1) \cdot 5(5-1) = 40$

(d) $\varphi(160) = \varphi(2^5 \cdot 5) = 2^4(2-1) \cdot (5-1) = 64$

Aufgabe 3.15

(a) 1 Generator (2) (b) 2 Generatoren (3 und 5)

Aufgabe 3.16

(a) in $\mathbb{Z}_5^*$: $3^1 = 3$, $3^2 = 4$, $3^3 = 2 \quad \Rightarrow \quad x = 3$

(b) in $\mathbb{Z}_{11}^*$: $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9 \quad \Rightarrow \quad x = 9$

(c) in $\mathbb{Z}_{23}^*$: $10^2 = 8$, $10^3 = 11$, $10^4 = 18 \quad \Rightarrow \quad x = 4$

Aufgabe 4.1

$\frac{21 \cdot 20}{2} = 210$ Schlüssel

Aufgabe 4.2

1. (a) Alice berechnet $A = 3^8 \mod 19 = 6$
   und sendet diese Zahl an Bob.

   (b) Bob berechnet $B = 3^7 \mod 19 = 2$
   und sendet diese Zahl an Alice.

2. (a) Alice berechnet $K_A = B^8 \mod 19 = 9$

   (b) Bob berechnet $K_B = A^7 \mod 19 = 9$

3. Alice und Bob können jetzt ihre Kommunikation mit dem gemeinsamen Schlüssel $K = 9$ verschlüsseln.

Aufgabe 4.3

Wenn es der Angreiferin Eve gelingt, sich in die Kommunikatin zwischen Alice und Bob einzuklinken, ist folgendes Szenario möglich:

- Eve kann sich die Primzahl p und das Element g beschaffen, da diese Zahlen öffentlich übertragen werden.
- Alice bildet die Zahl $A = g^a$ mit ihrem geheimen Exponenten a und sendet diese an Bob. Eve fängt A ab, bildet $E = g^e$ mit ihrem eigenen Exponenten e und sendet diesen Wert im Namen von Bob an Alice.
- Umgekehrt bildet Bob die Zahl $B = g^b$ mit seinem geheimen Exponenten b und sendet diese an Alice. Eve fängt B ab, bildet $E = g^e$ mit ihrem eigenen Exponenten e und sendet diesen Wert im Namen von Alice an Bob.
- Alice verschlüsselt die Nachricht m an Bob mit dem Schlüssel $K_{AE} = E^a = g^{ea}$, die Eve mit $K_{EA} = A^e = g^{ae}$ entschlüsselt. Eve kann jetzt die Nachricht lesen oder verändern. Die Nachricht m oder m' verschlüsselt sie mit dem Schlüssel $K_{EB} = B^e = g^{be}$, den sie mit Bob teilt und sendet sie an Bob. Dieser entschlüsselt die Nachricht mit $K_{BE} = E^b = g^{eb}$.

Diese Form von Angriff kann verhindert werden, indem die Datenpakete verschlüsselt werden. Dabei ist darauf zu achten, dass die Schlüssel über einen vertraulichen Kanal ausgetauscht werden oder dass sie eine vertrauenswürdige Stelle diese bestätigt. Andernfalls könnte

Aufgabe 5.1

(a)

a	b	$\lfloor a/b \rfloor$	x	y
21	9	2	1	-2
9	3	3	0	1
3	0	-	1	0

$3 = 1 \cdot 21 - 2 \cdot 9$

(b)

a	b	$\lfloor a/b \rfloor$	x	y
24	17	1	5	-7
17	7	2	-2	5
7	3	2	1	-2
3	1	3	0	1
1	0	-	1	0

$1 = 5 \cdot 24 - 7 \cdot 17$

(c)

a	b	$\lfloor a/b \rfloor$	x	y
38	34	1	-8	9
34	4	8	1	-8
4	2	2	0	1
2	0	-	1	0

$2 = (-8) \cdot 38 + 9 \cdot 34$

Aufgabe 5.2

(a)

a	b	x	y
11	5	1	-2
5	1	0	1
1	0	1	0

$5^{-1} = -2 = 9$ in $\mathbb{Z}_{11}^*$

(b)

a	b	x	y
12	7	3	-5
7	5	-2	3
5	2	1	-2
2	1	0	1
1	0	1	0

$7^{-1} = -5 = 7$ in $\mathbb{Z}_{12}^*$

(c)

a	b	x	y
17	9	-1	2
9	8	1	-1
8	1	0	1
1	0	1	0

$9^{-1} = 2$ in $\mathbb{Z}_{17}^*$

Aufgabe 5.3

$d = 23$

Aufgabe 5.4

$c = 15$

Aufgabe 5.5

$m = 24$

Aufgabe 5.5

Der verschlüsselte Text ist über eine Analyse der Zeichenhäufigkeiten angreifbar.

Aufgabe 5.6

Die Sicherheit des Verfahrens hängt davon ab, dass es (für deterministisch arbeitende Computer) keinen bekannten Algorithmus gibt, mit dem man Zahlen in weniger als exponentieller Zeit faktorisieren kann.

Darüber hinaus werden neue Computertypen erforscht (Quantencomputer, DNA-Computer), die teilweise nichtdeterministisch arbeiten und mit denen die Faktorisierungsaufgabe gelöst werden kann. Jedoch stecken diese Technologien in den Kinderschuhen und können keine Aufgaben realistischer Grössenordnungen lösen.

Schliesslich ist noch zu erwähnen, dass Computersystem oder Computernetzwerke der heutigen Zeit in der Lage sind bereits sehr grosse Faktorisierungsaufgaben zu lösen und dass daher die grösse des Schlüssels entscheidend für die Sicherheit des RSA-Verfahrens ist.