Aufgabe 1.1

Zähle stichwortartig die Hauptaufgaben der Kryptographie auf und beschreibe in einem Satz, worum es dabei jeweils geht.

Aufgabe 1.2

Wie viele Nachrichten der Länge 100 sind über einem Alphabet mit 4 Zeichen möglich?

Aufgabe 1.3

Was besagt das Prinzip von Kerckhoffs?

Aufgabe 1.4

Wie lautet der englische Fachausdruck für die die folgenden Form eines kryptografischen Angriffs?

(a) Ein Angreifer kann beliebigen Klartext verschlüsseln.

(b) Einem Angreifer ist bekannt, dass `GUTENTAG` zu `XMPTFTSU` verschlüsselt wird.

(c) Ein Angreifer kann beliebigen Geheimtext entschlüsseln.

Aufgabe 2.1

Dir folgende Geheimtext wurde bis auf die Leerzeichen mit einer Cäsar-Chiffrierung verschlüsselt.

`HEW AIXXIV MWX WGLSIR`

Bestimme den Klartext und den Schlüssel.

Aufgabe 2.2

Verschlüssle mit dem Vigenère-Quadrat:

Klartext: `GEHEIM`.

Schlüssel: `EFI`

Aufgabe 2.3

Entschlüssle den Geheimtext `WEEPZLSUHHWIEEIWIXHYXVZ`, der mit dem Schlüssel `TEMPO` und dem Vigenère-Verfahren chiffriert wurde.

Aufgabe 2.4

Wie geht man bei der Ciphertext-Attacke des Vigenère-Verfahrens vor?

Aufgabe 2.5

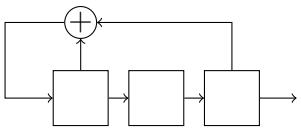
Der folgende Geheimtext ist durch eine Vigenère-Verschlüsselung entstanden. Bestimme die Schlüsselwortlänge.

Die Leerzeichen sind als „Lesehilfe“ eingefügt worden.

```
GNMCU TMXRM DNEWM IPUST YIHZK BNSIJ QOJZC ETOST QPRYQ MVPCM
YBOGR TFZSO WYFRZ MBBPS QKVNO DDMIP FCCPM TMWOY RVONP GTNLK
ZPIPS PKVNO CQRAZ GSTWW OKRTF PVJQO GPMVG VMVPV IOVKB RCION
OFTYX KZOGD TIXMX RPYRB QOZPV PKQXS FYXKZ XSSXI TWNSC ZVMIX
WDLXO WXSYH IXLOB PTRLI MVOPW CMQSY RINIM YEFQG TCGAC YTOLF
PEXLC OFHPM ZMBSL YKKZS TQPKK OOBMP WYMBS KTIRM QSYFX FBJIH
PVJMX SDCIO KRHOL WYASS PTRKV SBEPV TMDDC LIYMX NQFIN ZOBDZ
QAMCG PYWOM CWNSM TLOFL VYZMV ZPYYS OOPFY KAVKI DHIOK RZTNL
SQDRP CFXLB CSFRM LEFNS LGKUS CLYYM SBLYH KZCSE KIT
```

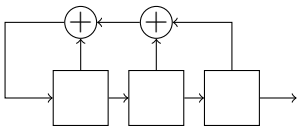
Aufgabe 2.6

Bestimme die Outputfolge des linearen rückgekoppelten Schieberegisters mit dem Anfangszustand [1, 0, 0].



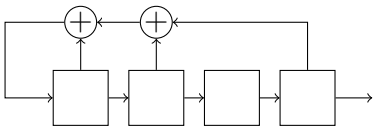
Aufgabe 2.7

Bestimme die Outputfolge des linearen rückgekoppelten Schieberegisters mit dem Anfangszustand [1, 1, 1].



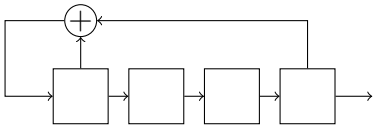
Aufgabe 2.8

Bestimme die Outputfolge des linearen rückgekoppelten Schieberegisters mit dem Anfangszustand [0, 1, 1, 0].



Aufgabe 2.9

Bestimme die Outputfolge des linearen rückgekoppelten Schieberegisters mit dem Anfangszustand [1, 0, 1, 1].



Aufgabe 3.1

Welche der folgenden Paare $(M, *)$ aus einer Menge M und einer Verknüpfung $*$ bilden eine Gruppe?

zur Erinnerung: $\mathbb{N} = \{1, 2, 3, \dots\}$, $\mathbb{N}_0 = \{0, 1, 2, \dots\}$

(a) $(\mathbb{N}_0, +)$ (c) $(\mathbb{Z}, +)$ (e) $(\mathbb{Q}, +)$ (g) $(\mathbb{R}, +)$

(b) $(\mathbb{N}, \cdot)$ (d) $(\mathbb{Z} \setminus \{0\}, \cdot)$ (f) $(\mathbb{Q} \setminus \{0\}, \cdot)$ (h) $(\mathbb{R} \setminus \{0\}, \cdot)$

Aufgabe 3.2

Wahr oder falsch?

(a) $3 \equiv 28 \mod 5$

(b) $28 \equiv 3 \mod 5$

(c) $-3 \equiv 28 \mod 5$

(d) $3 \equiv -28 \mod 5$

(e) $-3 \equiv -28 \mod 5$

(f) $-28 \equiv -3 \mod 5$

Aufgabe 3.3

(a) Stelle $(\mathbb{Z}_6, +)$ in Tabellenform dar.

(b) Handelt es sich um eine Gruppe?

Aufgabe 3.4

(a) Stelle $(\mathbb{Z}_6 \setminus \{0\}, \times)$ in Tabellenform dar.

(b) Handelt es sich um eine Gruppe?

Aufgabe 3.5

Stelle $\mathbb{Z}_8^*$ in Tabellenform dar.

Aufgabe 3.6

Berechne in $\mathbb{Z}_7$

(a) $5 + 6$ (b) $1 - 3$ (c) $3 \cdot 5$ (d) $1 : 4$ (e) $2 : 5$

Aufgabe 3.7

Bestimme die erzeugenden Elemente in $\mathbb{Z}_7^*$.

Aufgabe 3.8

Berechne die Potenzen in $\mathbb{Z}_{10}$.

(a) 1^{75}
(b) 2^{59}
(c) 3^{100}
(d) 4^{99}
(e) 5^{62}
(f) 6^{111}
(g) 7^{82}
(h) 8^{39}
(i) 9^{201}

Aufgabe 3.9

Berechne 2^{78} in $\mathbb{Z}_{17}$ mit dem Square-and-Multiply-Algorithmus.

Aufgabe 3.10

Berechne 14^{78} in $\mathbb{Z}_{17}$ mit dem Square-and-Multiply-Algorithmus. Verwende eine Multiplikationstafel.

Aufgabe 3.11

Berechne die Werte der eulerschen φ-Funktion. (p steht für eine beliebige Primzahl.)

(a) $\varphi(2)$
(b) $\varphi(3)$
(c) $\varphi(5)$
(d) $\varphi(7)$
(e) $\varphi(11)$
(f) $\varphi(p)$

Aufgabe 3.12

Prüfe nach, ob $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ für teilerfremde $a, b \in \mathbb{N}$ gilt.

(a) $a = 2$, $b = 3$
(b) $a = 3$, $b = 5$
(c) $a = 4$, $b = 5$
(d) $a = 7$, $b = 7$

Aufgabe 3.13

Berechne die Werte der eulerschen φ-Funktion. p ist eine beliebige Primzahl und $k \in \mathbb{N}$.

(a) $\varphi(4)$ (c) $\varphi(16)$ (e) $\varphi(9)$ (g) $\varphi(81)$

(b) $\varphi(8)$ (d) $\varphi(32)$ (f) $\varphi(27)$ (h) $\varphi(p^k)$

Aufgabe 3.14

Berechne $\varphi(n)$ mit Hilfe der Primfaktorzerlegung von n.

(a) $\varphi(24)$ (c) $\varphi(100)$

(b) $\varphi(36)$ (d) $\varphi(160)$

Aufgabe 3.15

Wie viele erzeugende Elemente hat die angegebene prime Resklassengruppe?

(a) $\mathbb{Z}_3$ (b) $\mathbb{Z}_7$

Aufgabe 3.16

Bestimme den diskreten Logarithmus in der angegebenen primen Restklassenmenge.

(a) $3^x = 2$ in $\mathbb{Z}_5^*$

(b) $2^x = 9$ in $\mathbb{Z}_{11}^*$

(c) $10^x = 18$ in $\mathbb{Z}_{23}^*$

Aufgabe 4.1

Wie viele Schlüssel sind bei einem symmetrischen Verschlüsselungsverfahren mit 21 Teilnehmern insgesamt nötig, wenn jeweils zwei Personen einen separaten gemeinsamen Schlüssel haben?

Aufgabe 4.2

Alice und Bob möchte eine verschlüsselt kommunzieren und haben folgende Vorbereitungen getroffen:

- Alice und Bob einigen sich auf die Primzahl $p = 19$ und die Primitivwurzel $g = 3$.
- Alice wählt zufällig $a = 8$ und Bob zufällig $b = 7$.

Beschreibe, wie die beiden einem gemeinsamen geheimen Schlüssel konstruieren können, ohne diesen vorher auf sicherem Wege ausgetauscht zu haben und berechne diesen gemeinsamen Schlüssel. Es darf davon ausgegangen werden, dass Alice und Bob sich gegenüber dem jeweils anderen authentifizieren konnten.

Aufgabe 4.3

Beschreibe, wie ein Man-in-the-Middle-Angriff auf den Diffie-Hellman-Schlüsselaustausch funktioniert und wie ihn Alice und Bob verhindern können.

Aufgabe 5.1

Stelle mit Hilfe des erweiterten euklidschen Algorithmus den grössten gemeinsamen Teiler der natürlchen Zahlen a und b als Linearkombination von a und b dar.

(a) $a = 21$ $b = 9$

(b) $a = 24$ $b = 17$

(c) $a = 38$ $b = 34$

Aufgabe 5.2

Bestimme die Inverse zum angegebenen Element in der primen Restklassengruppe mit Hilfe des erweiterten euklidschen Algorithmus.

(a) 5 in $\mathbb{Z}_{11}^*$

(b) 7 in $\mathbb{Z}_{12}^*$

(c) 9 in $\mathbb{Z}_{17}^*$

Aufgabe 5.3

Gegeben: Primzahlen $p = 5$ und $q = 11$ Berechne den privaten RSA-Schlüssel d aus dem öffentlichen RSA-Schlüssel $e = 7$.

Aufgabe 5.4

Verschlüssle die Nachricht $m = 9$ mit dem RSA-Verfahren und dem öffentlichen Schlüssel $(e, n) = (17, 33)$

Aufgabe 5.5

Entschlüssle die Nachricht $c = 24$ mit RSA-Verfahren und dem privaten Schlüssel $(d, n) = (9, 33)$.

Aufgabe 5.5

Jemand verschlüsselt jedes Zeichen einzeln mit dem RSA-Verfahren. Warum ist das unsicher?

Aufgabe 5.6

Erörtere die Sicherheit des RSA-Verfahrens.