Aufgabe 1.1

1. *Vertraulichkeit:* Nur berechtigte Personen sollen eine Nachricht lesen können.
2. *Authentizität:* Der Urheber einer Nachricht soll zweifelsfrei identifizierbar sein.
3. *Integrität:* Eine Nachricht soll vollständig und unverändert ankommen.
4. *Verbindlichkeit:* Der Empfänger kann beweisen, dass der Sender eine Nachricht mit identischem Inhalt verschickt hat.

Aufgabe 1.2

Die Sicherheit eines Kryptosystems darf nur von der Geheimhaltung des Schlüssels und nicht von der Geheimhaltung des Verfahrens abhängen.

Aufgabe 1.3

Die Untersuchung von Verschlüsselungsverfahren,

- um sie zu brechen („knacken“) oder …
- um ihre Sicherheit nachzuweisen.

Aufgabe 1.4

(a) Es steht das Verschlüsselungsverfahren zur Verfügung. (CP)

(b) Es steht ein Stück Geheimtext zur Verfügung. (KC)

(c) Es steht ein Stück Klartext und das dazu gehörende Stück Geheimtext zur Verfügung. (KP)

Aufgabe 2.1

Ein Verschlüsselungsverfahren, bei dem Sender und Empfänger den selben Schlüssel zum Ver- und Entschlüsseln verwenden.

Aufgabe 2.2

Auf 26! Arten.

Aufgabe 2.3

Der Hinweis deutet darauf hin, dass das Wort `KOLLEGI` in der Nachricht vorkommen könnte. In der Tat besteht das Geheimtextwort `NROOHJL` aus 7 Zeichen. Somit könnte der Geheimtextbuchstabe `N` aus dem Klartextbuchstaben `k` hervorgegangen sein, was eine zyklische Verschiebung um +3 Zeichen bedeutet. Wendet man diese Verschiebung auf den gesamten Text an, erhält man in der Tat:

`EIN UHR BEIM KOLLEGI`

Der Hinweis ist natürlich wichtig, wenn wir nicht maximal 25-mal probieren wollen.

Aufgabe 2.5

Weil durch das Ersetzen der einzelnen Buchstaben die für eine Sprache charakteristischen Zeichenhäufigkeiten erhalten bleiben. So können bei genügend langen Geheimtexten einige Buchstaben mit hoher Wahrscheinlichkeit richtig ersetzt werden. Danach können die übrigen Zeichen aus dem Zusammenhang erraten werden.

Die folgenden Daten müssen für die Prüfung nicht gelernt werden, sind aber trotzdem interessant:

	Deutsch	Englisch	Französisch
häufigster Buchstabe	e (18%)	e (12%)	e (16%)
zweithäufigster Buchstabe	n (11%)	t (10%)	a (9%)
dritthäufigster Buchstabe	i (8%)	a (8%)	i (8%)

http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/1_Monoalph/lang.html (23.5.2012)

Aufgabe 2.6

Klartextbuchstaben	K	A	F	F	E	E
Schlüsselbuchstaben	G	E	H	E	I	M
Geheimtextbuchstaben	Q	E	M	J	M	Q

Siehe auch: `http://einklich.net/etc/vigenere.htm`

Aufgabe 2.7

Falls das Schlüsselwort nicht so lange wie der Text ist muss es zur Verschlüsselung wiederholt werden. Je öfter aber das Schlüsselwort wiederholt wird, desto wahrscheinlicher wird es, ein Wort, das an mehreren Stellen im Klartext vorkommt auch durch dasselbe Geheimtextwort verschlüsselt wird.

Deshalb sollte man nach identischen Folgen von Geheimtextstücken suchen. Der Abstand zwischen zwei dieser Zeichenfolgen muss dann ein Vielfaches der Schlüsselwortlänge sein. Findet man mehr als zwei dieser Übereinstimmungen, bildet man den grössten gemeinsamen Teiler der Abstände.

Dieses Verfahren wird übrigens *Kasiski-Test* genannt (der Ausdruck gehört aber nicht zum Prüfungsstoff)

Aufgabe 2.8

Jeweils eine separate Zeichenhäufigkeitsanalyse an den folgenden Stellen durchführen:

- $1,\ n+1,\ 2n+1,\ \ldots$
- $2,\ n+2,\ 2n+2,\ \ldots$
- $\ldots,$
- $n-1,\ 2n-1,\ 3n-1,\ \ldots$
- $n,\ 2n,\ 3n,\ \ldots$

Aufgabe 2.9

(a)
- Es müssen auf Vorrat grosse Schlüssel erzeugt und ausgetauscht werden.
- Die Zufallszahlen der Schlüssel sollten von hoher Qualität sein.

(b)
- Dass ein Schlüssel höchstens einmal verwendet wird.
- Dass die verwendeten (Pseudo-)Zufallszahlen sicher sind, d. h. dass sie sich nicht von einer echten Zufallszahlenfolge unterscheiden und dass der Anfangszustand der Folge nicht erraten werden kann.

Aufgabe 3.1

(a) $113 \equiv 17 \mod 8$ wahr

(b) $-352\,989 \equiv 724\,692 \mod 2$ falsch

(c) $107\,032 \equiv 0 \mod 3$ wahr [Quersummenregel]

Aufgabe 3.2

(a) $7 + 6 = 4$

(b) $5 - 8 = 6$

(c) $3 \cdot 7 = 3$

(d) $1 : 4 = 1 \cdot 7 = 7$

(e) $5 : 6$ nicht definiert, da 6 in $\mathbb{Z}_9$ kein Inverses hat

(f) $3^2 = 0,\ 3^3 = 0,\ \ldots,\ 3^{29} = 0$

Aufgabe 3.3

Die Modulo-Operation kann mit der Addition und der Multiplikation vertauscht werden. Damit das Endresultat auch kleiner als das Modul wird, muss in der Regel am Schluss noch ein zusätzliche Modulo-Rechnung durchgeführt werden.

$$
\begin{aligned}
&(25 \cdot 13 + 44 \cdot 8) \mod 7\\
&= \big[(25 \mod 7) \cdot (13 \mod 7) + (44 \mod 7) \cdot (8 \mod 7)\big] \mod 7\\
&= \big[4 \cdot 6 + 2 \cdot 1\big] \mod 7\\
&= 26 \mod 7 = 5
\end{aligned}
$$

Aufgabe 3.4

$+$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

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

Aufgabe 3.5

(a) $(\mathbb{Z}_8, +)$ ja

(b) $(\mathbb{Z}_5, \times)$ nein, denn 0^{-1} existiert nicht

(c) $(\mathbb{Z}_7 \setminus \{0\}, \times)$ ja

(d) $(\mathbb{Z}_6 \setminus \{0\}, \times)$ nein denn 2^{-1}, 3^{-1} und 4^{-1} existieren nicht

Aufgabe 3.6

Die prime Restklassengruppe $\mathbb{Z}_n^*$ ist immer multiplikativ definiert, weshalb man dafür nicht extra $(\mathbb{Z}_n^*, \times)$ schreibt.

$\mathbb{Z}_{12}^*$ besteht aus allen Elementen, die invertierbar sind und dies sind genau die die zu 12 teilerfremden Elemente.

$\times$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Aufgabe 3.7

(a) $g = 3$, $(\mathbb{Z}_4, +)$

ja, denn durch wiederholtes Addieren von 3 mit sich selbst, wird die gesamte Menge $\mathbb{Z}_4$ durchlaufen:

$3,\ 3 + 3 = 2,\ 3 + 3 + 3 = 1,\ 3 + 3 + 3 + 3 = 0,\ \ldots$

(b) $g = 2$, $(\mathbb{Z}_6, \times)$

nein, denn durch wiederholtes Multiplizieren von 2 mit sich, wird nicht die gesamte Menge $\mathbb{Z}_6$ durchlaufen:

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 2,\ 2^4 = 4,\ \ldots$

(c) $g = 3$, $(\mathbb{Z}_5^*, \times)$

ja, denn durch wiederholtes Multiplizieren von 3 mit sich selbst, wird die gesamte Menge $\mathbb{Z}_5$ durchlaufen:

$3^1 = 3,\ 3^2 = 4,\ 3^3 = 2,\ 3^4 = 1,\ 3^5 = 3,\ \ldots$

Aufgabe 3.8

$\varphi(n)$ ist die Menge aller zu n teilerfremden Zahlen $k < n$. Ist n eine Primzahl, so sind alle natürlichen Zahlen $k < n$ teilerfremd zu n und es gilt $\varphi(n) = n - 1$.

(a) $\varphi(8) = 4$

(b) $\varphi(11) = 11$

(c) $\varphi(24) = 8$

(d) $\varphi(47) = 46$

Aufgabe 3.9

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

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

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

$\times$	**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)
$$\begin{array}{ll} 10 = 2 \cdot 5 & 14^2 = 6 \\ 5 = 2 \cdot 2 + 1 & 13 \cdot 17^2 = 14 \\ 2 = 2 \cdot 1 & 13^2 = 17 \\ 1 = 2 \cdot 0 + 1 & 13 \cdot 1^2 = 13 \end{array}$$

(b)
$$\begin{array}{ll} 16 = 2 \cdot 8 & 6^2 = 17 \\ 8 = 2 \cdot 4 & 5^2 = 6 \\ 4 = 2 \cdot 2 & 9^2 = 5 \\ 2 = 2 \cdot 1 & 3^2 = 9 \\ 1 = 2 \cdot 0 + 1 & 3 \cdot 1^2 = 3 \end{array}$$

Aufgabe 3.14

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

Aufgabe 3.15

Beim DHM-Schlüsselaustausch 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

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

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

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

(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

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

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:

$$\begin{array}{ll} 7 = 2 \cdot 3 + 1 & 10 \cdot 10^2 = 10 \\ 3 = 2 \cdot 1 + 1 & 10 \cdot 10^2 = 10 \\ 1 = 2 \cdot 0 + 1 & 10 \cdot 1^2 = 10 \end{array}$$

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

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

$$\begin{array}{ll} 7 = 2 \cdot 3 + 1 & 5 \cdot 26^2 = 14 \\ 3 = 2 \cdot 1 + 1 & 5 \cdot 5^2 = 26 \\ 1 = 2 \cdot 0 + 1 & 5 \cdot 1^2 = 5 \end{array}$$

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

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)