Aufgabe 1.1

1. *Vertraulichkeit:* Nur berechtigte Personen sollen eine Nachricht lesen können.
2. *Authentifikation:* 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) $\varphi(47) = 46$