Aufgabe 1

Was ist Kryptologie und mit welchen Teildisziplinen befasst sie sich?

Aufgabe 2

Skizziere schematisch die Situation, in der sich zwei Kommunikationspartner befinden, die eine vertauliche Informationen austauschen wollen.

Aufgabe 3

Beschreibe das Prinzip von Kerckhoffs.

Aufgabe 4

Was ist das charakteristische Merkmal symmetrischer kryptographischer Verfahren?

Aufgabe 5

(a) Was ist eine monoalphabetische Substitutionschiffre?

(b) Erörtere die Sicherheit dieser Art der Verschlüsselung?

Aufgabe 6

Nennen Sie ein Beispiel für eine monographisch-monoalphabetische Substitutionschiffre.

Aufgabe 7

Was ist eine polyalphabetische Substitutionschiffre?

Aufgabe 29

Sie kommen in den Besitz des folgenden Geheimtexts, von dem Sie wissen, dass er mit dem Vigenère-Verfahren verschlüsselt wurde.

```
01234567890123456789012345 67
PHSRMZNHZHSRMZRIVQXWVQLSAHSR
```

Die über den Zeichen stehenden Ziffern dienen dazu, die Zeichenpositionen leichter erkennbar zu machen.

Ermitteln Sie die Kandidaten für die Schlüsselwortlänge.

Aufgabe 9

Beschreiben Sie die Vigenère-Chiffere und diskutieren Sie ihre Sicherheit.

Aufgabe 10

Beschreiben Sie das One-Time-Pad-Verfahren und diskutieren Sie dessen Sicherheit.

Aufgabe 11

Wandle die Nachricht $m =$ `MMS` gemäss folgender Codetabelle in eine Bitfolge um, verschlüssele sie durch `XOR`-Verknüpfung mit dem Schlüssel $k =$ `110111111001001` und stelle den Geheimtext wieder mit den urspünglichen Zeichen dar.

A=00000	B=00001	C=00010	D=00011
E=00100	F=00101	G=00110	H=00111
I=01000	J=01001	K=01010	L=01011
M=01100	N=01101	O=01110	P=01111
Q=10000	R=10001	S=10010	T=10011
U=10100	V=10101	W=10110	X=10111
Y=11000	Z=11001	!=11010	?=11011
+=11100	*=11101	@=11110	#=11111

Aufgabe 30

Verschlüssle den Text `BRUTUSISTDERVERRAETER` mit der Transpositionschiffre und dem Schlüsselwort `ANANAS`.

Aufgabe 31

Du hast mit jemandem das Schlüsselwort `HAMSTER` vereinbart und bekommst den Geheimtext

`RMAEF TALED TNPFO ZFR`

der mit der einfachen Transpositionschiffre verschlüsselt wurde. Zur Verschleierung der Schlüsselwortlänge wurden die Zeichen des Geheimtexts in 5er-Gruppen gegliedert.

Entschlüssle die Nachricht und bestimme den Treffpunkt.

Aufgabe 16

Beschreibe das Konzept asymmetrischer Kryptosysteme.

Aufgabe 19

Stelle $(\mathbb{Z}_6, \times)$ tabellarisch dar. Welche Elemente in $(\mathbb{Z}_6, \times)$ sind invertierbar?

Aufgabe 20

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

Aufgabe 22

Prüfe, ob

(a) $a = 2$

(b) $b = 3$

ein Generator von $\mathbb{Z}_7$ ist.

Aufgabe 23

(a) Löse die Gleichung $2^a = 1$ in $\mathbb{Z}_5$.

(b) Wie wird die Lösung dieser Art von Gleichung genannt?

Aufgabe 24

Berechne 3^9 mod 11 mit Square and Multiply.

Aufgabe 25

Erkläre, wie der Diffie-Hellman-Merkle-Schlüsselaustausch funktioniert und worin seine Sicherheit besteht.

Aufgabe 26

Alice und Bob einigen sich auf die Primzahl $p = 17$ und den Generator $g = 10$. Alice wählt die Zahl $a = 2$ und Bob die Zahl $b = 16$. Wie lautet der gemeinsame Schlüssel aufgrund des Diffie-Hellman-Schlüsselautauschprotokolls?

Verwende den Taschenrechner so weit es geht.