

Aufgabe 1

d	i	e	a	x	t	i	m	h	a
M	B	P	D	U	I	B	N	Y	D
u	s	e	r	s	p	a	r	t	d
L	F	P	C	F	W	D	C	I	M
e	n	z	i	m	m	e	r	m	a
P	Q	A	B	N	N	P	C	N	D
n	n								
Q	Q								

Quelltext des verwendeten Programms angefügt

$d = (3 \cdot 3 + 3) \bmod 26 = 12$
 $i = (3 \cdot 8 + 3) \bmod 26 = 1$
 $e = (3 \cdot 4 + 3) \bmod 26 = 15$
 $a = (3 \cdot 0 + 3) \bmod 26 = 3$
 $x = (3 \cdot 23 + 3) \bmod 26 = 20$
 $t = (3 \cdot 19 + 3) \bmod 26 = 8$
 $m = (3 \cdot 12 + 3) \bmod 26 = 13$
 $h = (3 \cdot 7 + 3) \bmod 26 = 24$
 $u = (3 \cdot 20 + 3) \bmod 26 = 11$
 $s = (3 \cdot 18 + 3) \bmod 26 = 5$
 $r = (3 \cdot 17 + 3) \bmod 26 = 2$
 $n = (3 \cdot 13 + 3) \bmod 26 = 16$
 $p = (3 \cdot 15 + 3) \bmod 26 = 22$
 $z = (3 \cdot 25 + 3) \bmod 26 = 0$

Aufgabe 2

Da „z“ sehr häufig vorkommt, müsste es einen Vokal abbilden. Wenn man die Verschiebechiffre darauf anwendet, kommt kein sinnvoller Klartext raus. Als nächstes wurde der Atbash verwendet, wobei als Lösung herauskam:

Time flies like an arrow fruit flies like a banana

Aufgabe 3

$$\begin{aligned}
 [a]_m \cdot ([b]_m + [c]_m) &= [a]_m \cdot [(b+c)]_m \\
 &= [a \cdot (b+c)]_m \\
 &= [a \cdot b + a \cdot c]_m \\
 &= [a \cdot b]_m + [a \cdot c]_m \\
 &= [a]_m \cdot [b]_m + [a]_m \cdot [c]_m
 \end{aligned}$$

Aufgabe 4

1. Falsch,
Beispiel:

$$\begin{aligned}
 a = 2 \quad b = 3 \quad c = 6 \\
 ggT(a, b, c) &= 1 \\
 ggT(a, b) &= 1 \\
 ggT(a, c) &= 2 \\
 ggT(b, c) &= 3
 \end{aligned}$$

2. Richtig,

Beweis durch Widerspruch:

Es gelte $ggT(a, b) = 1 \vee ggT(a, c) = 1 \vee ggT(b, c) = 1$ und $ggT(a, b, c) \neq 1$

$$\begin{aligned}
 ggT(a, b, c) \neq 1 &\Rightarrow \exists n \in \mathbb{N} \setminus \{0, 1\} : n|a \wedge n|b \wedge n|c \\
 &\Rightarrow ggT(a, b) \geq n \wedge ggT(a, c) \geq n \wedge ggT(b, c) \geq n
 \end{aligned}$$

Was im Widerspruch zur Annahme steht, somit folgt $ggT(a, b) = 1 \vee ggT(a, c) = 1 \vee ggT(b, c) = 1 \Rightarrow ggT(a, b, c) = 1$

Aufgabe 5

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

(\mathbb{Z}_8^*, \cdot)	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1