

Dr. T. Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 426
0531 391-7527



Übungsblatt 1

Aufgabe 1. (Multiplikative Chiffren und Tauschchiffren)

- Für $k \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ ist die Multiplikation mit k modulo 26 eine multiplikative Chiffre. Gibt es Buchstaben, die unter jeder dieser Chiffren fest bleiben?
- Zeigen Sie: Die Multiplikation mit a modulo n ist umkehrbar, genau dann wenn $\text{ggT}(a, n) = 1$ ist.
- Entschlüsseln Sie den Geheimtext **WKDUIQ**, wenn Sie wissen, dass eine Tauschchiffre mit einem Schlüssel der Form $(7, t)$ verwendet wurde. Tipp: Es handelt sich um einen weiblichen Vornamen. Erinnern Sie sich dazu, dass die Entschlüsselung eines Geheimbuchstaben c für eine Tauschchiffre mit Schlüssel (s, t) durch $D_{(s,t)}(c) = s^{-1}(c - t)$ gegeben ist.
- Entschlüsseln Sie den Geheimtext **PZUVFH**, wenn Sie wissen, dass eine Tauschchiffre mit einem Schlüssel der Form $(s, 7)$ verwendet wurde. Tipp: Es handelt sich um einen weiblichen Vornamen.

Aufgabe 2. (Monoalphabetische Chiffren)

Entschlüsseln Sie folgenden Geheimtext, der mit einer monoalphabetischen Chiffre verschlüsselt wurde. Es handelt sich um einen Text in deutscher Sprache.

YZBYY ZBKJY NGJBO ZBXZY MZHYY BHWNU KILCA LYGHW
NTJYH HYTBL YGVYG OYBJB XLYGN YZATZ WNYBC NBYUT
TYOYN YZABZ HRGUY AYGYZ UVYGB ZWNIC NBYNZ BIYGT
ZHIZO YBHWN UTRXU GOYHI YTTIS JABJI SYBJB XYGOC
YISYB XYHUT TOYAY ZBYBD JVTZR JAH

Hilfsmittel: Identifikation der Buchstaben a-z mit den Ziffern 0-25.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25