

## Aufgaben: Zahlentheorie

### Teil 2.2: Einfache Kryptoverfahren auf Basis des modularen Rechnens

---

#### Aufgabe 1.

Eine einfache Art, einen Text zu chiffrieren, ist die **Caesar-Verschlüsselung**. Bei ihr erhält man den verschlüsselten Buchstaben im Wesentlichen dadurch, dass man ihn durch einen im Alphabet verschobenen ersetzt. Beschreiben lässt sich das wie folgt:

- Wir ersetzen jeden Buchstaben durch seine Stelle im Alphabet:  $A = 1, B = 2, \dots, Z = 26$
- Der Schlüssel  $s$  gibt die Anzahl der Stellen wieder, um die wir verschieben (dabei ist  $s > 0$  oder  $s < 0$  abhängig davon, ob wir nach rechts oder nach links verschieben).

Entspricht  $x$  dem Buchstaben der Originalnachricht, dann entspricht  $y \equiv x + s \pmod{26}$  dem Buchstaben der chiffrierten Nachricht.

- a) Verschlüsseln Sie den Text "Das Kaninchen versteckt sich in seinem Bau" mit  $s = 5$ .
- b) Begründen Sie, warum die Gleichung  $x \equiv y - s \pmod{26}$  geeignet ist, um den verschlüsselten Text zu decodieren.
- c) Entschlüsseln Sie den Text, der mit  $s = 5$  verschlüsselt wurde: "ijw kzhmx bfwyjj atw ijr ggz".
- d) Begründen Sie, warum die Verschlüsselungen mit den Schlüsseln  $s$  und  $s' = -(26 - s) < 0$  für  $0 < s < 26$  das gleiche Resultat liefern.
- e) Erläutern Sie, was das Besondere an der Verschlüsselung mit  $s = 13$  ist? Diese spezielle Art der Caesar-Verschlüsselung nennt man **ROT13**.

#### Aufgabe 2.

Das achtstellige Geburtsdatum  $z_1 z_2 . z_3 z_4 . z_5 z_6 z_7 z_8$  einer Person wird innerhalb einer Behörde verschlüsselt weitergeleitet. Dazu wird jede Ziffer des Datums mit Hilfe der Formel

$$y_i \equiv 3 \cdot z_i \pmod{10}$$

codiert.

- a) Codieren Sie das Datum 17.03.1984.

---

Adresse: Eduard-Spranger-Berufskolleg, 59067 Hamm

E-Mail: [mail@frank-klinker.de](mailto:mail@frank-klinker.de)

Version: 12. März 2025

- b) Begründen Sie im Detail, warum  $z_i \equiv 7 \cdot y_i \pmod{10}$  die Formel zum Entschlüsseln der Daten ist.
- c) Entschlüsseln Sie 32023714.
- d) Warum ist die Formel  $y_i = 4 \cdot z_i \pmod{10}$  nicht zum Verschlüsseln geeignet.
- e) Welche Eigenschaft muss die Zahl  $a$  mindestens besitzen, damit  $y_i = a \cdot z_i \pmod{10}$  zum Verschlüsseln verwendet werden kann.