Frank Klinker

Aufgaben: Zahlentheorie

Teil 2.2: Einfache Kryptoverfahren

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: $A = 1, B = 2, \ldots, Z = 26$
- Der Schlüssel s gibt die Anzahl der Stellen wieder, um die wir verschieben (dabei ist $e > 0$ oder $e < 0$ abhängig davon, ob wir nach rechts oder nach links verschieben).

Entspricht x dem Buchstaben der Originalnachricht, dann entspricht $y \equiv x + s \mod 26$ 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 $x \equiv y - s \mod 26$ geeignet ist, um den verschlüsselten Text zu decodieren?

c) Entschlüsseln Sie den Text, der mit $e = s$ verschlüsselt wurde: *ijw kzhmx bfwyjy atw ijr gfz.*

d) Begründen Sie, warum die Verschlüsselungen mit dem Schlüssel $0 < s < 26$ und $s' = -(26 - s) < 0$ das gleiche Resultat liefern?

e) Was ist das besondere an der Verschlüsselung mit $s = 13$? Diese spezielle Arte 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

$$y_i \equiv 3 \cdot z_i \mod 10$$

codiert.

a) Codieren Sie das Datum 17.03.1984.

b) Begründen Sie im Detail, warum $z_i \equiv 7 \cdot y_i \mod 10$ die Formel zum Entschlüsseln der Daten ist.

Adresse: Eduard-Spranger-Berufskolleg, 59067 Hamm
E-Mail: mail@frank-klinker.de
Version: 5. Juni 2024

c) Entschlüsseln Sie 32023714.

d) Warum ist die Formel $y_i = 4 \cdot z_i \mod 10$ nicht zum Verschlüsseln geeignet.

e) Welche Eigenschaft muss die Zahl a mindestens besitzen, damit $y_i = a \cdot z_i \mod 10$ zum Verschlüsseln verwendet werden kann.