FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
11.10.2023

Musterlösung zum 2. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Die Menge ist eine Gruppe. Dazu muss man sich folgendes überlegen:

- Die Hintereinanderausführung zweier Vigenère-Verschlüsselungen ergibt wieder eine Vigenère-Verschlüsselungen:

  Betrachtet man die Vigenère-Verschlüsselung als positionsweise Addition modulo 26 mit den (periodischen) Schlüssel-Buchstaben, so sieht man, dass eine Hintereinanderausführung auch eine positionsweise Addition modulo 26 ist. Dabei ergibt sich eine Periode mit einer Länge gleich dem kleinsten gemeinsamen Vielfachen der einzelnen Perioden, z.B. bei Verkettung von Vigenère-Verschlüsselungen mit den Schlüsseln und BETA und GUSTAV der Längen 4 und 6 ergibt sich das 12 Zeichen lange Schlüsselwort HYLTBZZUTXTV:

  ```
  Schlüssel 1: B E T A|B E T A|B E T A|B E T A|B E T A|...
  Schlüssel 2: G U S T A V|G U S T A V|G U S T A V|G U S T A V|...
  zusammen   : H Y L T B Z Z U T X T V|H Y L T B Z Z U T X T V|...
  ```

- Die Hintereinanderausführung ist assoziativ.

  Dies gilt allgemein bei Abbildungen, vgl. Zusatzaufgabe von Blatt 1.

- Es gibt ein neutrales Element.

  Das neutrale Element ist die „Verschlüsselung“, die nichts ändert, hier die Verschlüsselung mit dem einbuchstabigen Schlüsselwort A.

- Es gibt inverse Elemente.

  Das inverse Element muss die ursprüngliche Verschlüsselung rückgängig machen.

  Bei der Vigenère-Verschlüsselung gibt es zu einem Schlüsselwort ein entsprechendes „Entschlüsselwort“, indem jeweils der zum entsprechenden Schlüsselwort-Buchstaben „inverse“ Buchstaben (bei Interpretation als Zahl zum Buchstaben k der Buchstabe $26-k$) genommen wird; beispielsweise ist zum Schlüsselwort BETA das Entschlüsselungswort ZWHA.

Die Menge der Vigenère-Verschlüsselungen ist sogar kommutativ, da man die Verschlüsselung jeweils als Addition von als Zahlen interpretierte Buchstaben auffassen kann, und bei diesen Additionen die Reihenfolge keine Rolle spielt.

Übung 2

a) In $\mathbb{Z}_{20}$ mit „$\oplus$“ ist $\overline{15} = 5$ das inverse Element zu 15. Also:

$$15 \oplus x \;=\; 2 \bmod 20 \;\Rightarrow\; 5 \oplus 15 \oplus x \;=\; 5 \oplus 2 \bmod 20 \;\Rightarrow\; x \;=\; 7 \bmod 20.$$

b) In $\mathbb{Z}_5 \setminus \{0\}$ ist $\bar{3} = 2$. Also:

$$3 \cdot x \;=\; 4 \bmod 5 \;\Rightarrow\; 2 \cdot 3 \cdot x \;=\; 2 \cdot 4 \bmod 5 \;\Rightarrow\; x \;=\; 8 \;=\; 3 \bmod 5$$

c) Das inverse Element zu A ist $A^{-1} = \frac{1}{1 \cdot 5 - 2 \cdot 3} \cdot \left(\begin{smallmatrix} 5 & -3 \\ -2 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -5 & 3 \\ 2 & -1 \end{smallmatrix}\right)$. Also:

$$A \cdot X \;=\; \begin{pmatrix} 2 & -1 \\ 4 & 0 \end{pmatrix} \quad\Rightarrow\quad A^{-1} \cdot A \cdot X \;=\; A^{-1} \cdot \begin{pmatrix} 2 & -1 \\ 4 & 0 \end{pmatrix}$$

$$\Rightarrow\; X \;=\; \begin{pmatrix} -5 & 3 \\ 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 \\ 4 & 0 \end{pmatrix} \;=\; \begin{pmatrix} 2 & 5 \\ 0 & -2 \end{pmatrix}.$$

Übung 3

a) In $\mathbb{Z}_5 \setminus \{0\}$ ist

$$1 = a^4 = a \odot a \odot a \odot a = (a \cdot a \cdot a \cdot a) \bmod 5 = a^4 \bmod 5,$$

z.B. $2^4 = 16 = 1 \bmod 5$.

Für $\mathbb{Z}_7 \setminus \{0\}$ folgt entsprechend $a^6 = 1 \bmod 7$, z.B. $4^6 = 4096 = 1 \bmod 7$.

b)
- Caesar-Verschiebungen

  Die Gruppe der Caesar-Verschiebungen hat 26 Elemente. Satz 1.3. besagt daher, dass nach einer 26-fachen Wiederholung der gleichen Caesar-Verschiebung wieder der Klartext erscheint.

  (Dies ist auch direkt ersichtlich, wenn man die Verschiebung als Addition einer Klartextzahl k mit einer Verschiebung v modulo 26 betrachtet. Die 26-fache Wiederholung bringt dann $k + 26v \bmod 26 = k$.)

- Monoalphabetische Verschlüsselung

  Es gibt insgesamt 26! viele monoalphabetische Verschlüsselungen. Nach Satz 1.3. erhält man also nach einer 26!-fachen Wiederholung einer immer gleichen monoalphabetischen Verschlüsselung wieder den Klartext.

  (Tatsächlich gibt es zu jeder monoalphabetischen Verschlüsselung schon eine viel geringere Wiederholungszahl, bei der der Klartext erscheint.)

- Vigenère-Verschlüsselung

  Da die Länge eines Vigenère-Schlüsselwortes beliebig lang sein kann, ist die Menge aller Vigenère-Verschlüsselungen unendlich, so dass Satz 1.3. nicht direkt anwendbar ist. Man kann aber die Menge aller Vigenère-Verschlüsselungen zu Schlüsselworten einer festen Länge L betrachten, z.B. die zu fünf Buchstaben

langen Schlüsselworten. Man kann sich leicht überlegen, dass diese Menge eine Gruppe ist mit 26^L vielen Elementen. Satz 1.3. besagt daher, dass nach einer 26^L-fachen Wiederholung einer Vigenère-Verschlüsselung mit einem Schlüsselwort der Länge L der Klartext erscheint.

(Tatsächlich erhält man sogar schon bei einer 26-fachen Wiederholung den Klartext, denn dann hat man zu jedem Buchstaben eine 26-fache Caesar-Verschiebung durchgeführt, die wieder den Klartextbuchstaben ergibt, s.o..)

Zusatzaufgabe

Sei ■ das neutrale Element. Dann ist die Verknüpfungstafel schon wie folgt festgelegt:

∘	■	★	▲
■	■	★	▲
★	★		
▲	▲		

Da in jeder Zeile und Spalte jedes Element vorkommen muss, würde sowohl ★ ∘ ★ = ★ also auch ★∘★ = ■ zu einem Widerspruch führen (im letzeren Fall müsste dann ★∘▲ = ▲ sein), also muss ★ ∘ ★ = ▲ und damit ergibt sich der Rest, so dass man erhält:

∘	■	★	▲
■	■	★	▲
★	★	▲	■
▲	▲	■	★

Nach Festlegung des neutralen Elements ist die Verknüpfungstafel also eindeutig.