Diskrete Mathematik für Lehramt Informatik
Sommersemester 2021

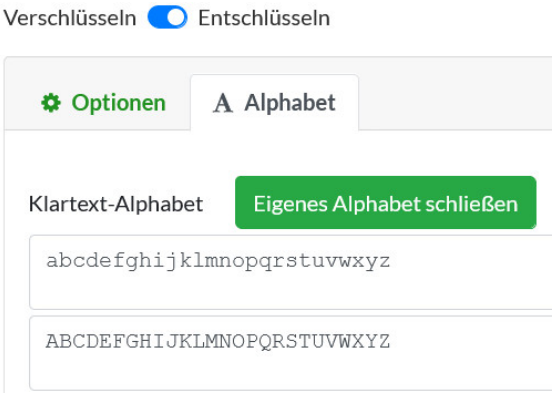
11. Übungsblatt (17.6.2021)

In den Beispielen 11.1, 11.2 und 11.3 sind Computerprogramme zum Entschlüsseln der Texte explizit zugelassen. Zum Vorrechnen in der Übungseinheit sollten Sie das Verwenden des Programmes zeigen (z.B. durch Teilen des Bildschirms). Leer- und Satzzeichen bleiben in allen Beispielen durch die jeweilige Verschlüsselung unverändert. Umlaute und ß wurden jeweils als `AE`, `OE`, `UE` *bzw.* `SS` *ausgeschrieben.*

Beispiel 11.1. Der folgende Text wurde mit einer Caesar Chiffre verschlüsselt. Erraten Sie den Schlüssel per Hand, indem Sie sich das erste Wort des Textes ansehen. Verwenden Sie anschließend ein Computerprogramm (z.B. `https://www.cryptool.org/de/cto/caesar`), um den kompletten Text zu entschlüsseln.
QVRFRE NOFNGM JHEQR QHEPU RVARA PNRFNE PUVSSER ZVG IREFPUHO QERVMRUA IREFPUYHRFFRYG. QVRFR IREFPUYHRFFRYHAT UNG QVR ORFBAQREURVG, QNFF QVR IREFPUYHRFFRYHAT HAQ RAGFPUYHRFFRYHAT QVR TYRVPUR SHAXGVBA IREJRAQRA.

Beispiel 11.2. Für den Text auf der nächsten Seite wurde eine monoalphabetische Verschlüsselung verwendet. Ermitteln Sie mit Computerhilfe die Häufigkeit der Buchstaben im verschlüsselten Text (z.B. `https://www.cryptool.org/de/cto/frequency-analysis`). Entschlüsseln Sie danach mit `https://www.cryptool.org/de/cto/monoalpha` den Text:

- Kopieren Sie den verschlüsselten Text in das Feld „Eingabe“.
- Stellen Sie den Schieberegler auf „Entschlüsseln“.
- Klicken Sie darunter auf „Alphabet“ und „Eigenes Alphabet definieren“ und geben Sie Klartext- und Geheimtext-Alphabet wie im nachfolgenden Screenshot an. Dadurch werden zunächst alle Buchstaben in Kleinbuchstaben übersetzt.



- Ersetzen Sie im Klartext-Alphabet den häufigsten Buchstaben des verschlüsselten Textes durch den Großbuchstaben E und den zweithäufigsten Buchstaben durch N.
- Versuchen Sie, die weiteren Buchstaben anhand der Häufigkeit der Buchstaben und einzelner Worte im Text zu erraten und tragen Sie diese Buchstaben nach und nach im Klartext-Alphabet ein.

XVGX ZFFWXTXVGX TSGSZFHDZAXJVQYDX KXIQYDFPXQQXFPGW VQJ GVYDJ XVGCZYD HXI DZGB MP XIIZJXG. MPQZXJMFVYD MP XVGXI DZXPCVWUXVJQZGZFNQX UZGG TZG ZPYD BVX DZXPCVWUXVJ BXI APYDQJZAXG ZG BXG EXOXVFVWXG HSQVJVSGXG VT OSIJ AXJIZYDJXG. OZXDIXGB VG BXPJQYDXG JXLJXG X BXI DZXPCVWQJX APYDQJZAX VQJ, VQJ B BXI DZXPCVWQJX ZGCZGWQAPYDQJZAX PGB G BXI DZXPCVWQJX XGBAPYDQJZAX KSG OSXIJXIG.

Beispiel 11.3. Eine Weiterentwicklung der Caesar Chiffre ist die Vigenère Chiffre. Bei dieser Verschlüsselung werden mehrere Zahlen $k_1, k_2, \ldots, k_r$ gewählt und dann der erste Buchstabe im Text wie bei der Caesar Chiffre um k_1 verschoben, der zweite Buchstabe um k_2 und so weiter. Nach den ersten r Buchstaben beginnt man wieder von vorne; der $(r+1)$-te Buchstabe wird also um k_1 verschoben, der $(r+2)$-te Buchstabe um k_2 etc. Die Zahlen $k_1, k_2, \ldots, k_r$ werden dabei meist also Buchstaben dargestellt (A $\leftrightarrow$ 0, B $\leftrightarrow$ 1 etc.) und bilden somit ein Schlüsselwort.

Der unten stehende Text wurde durch einen Schlüssel der Länge 2 verschlüsselt. Verwenden Sie `https://www.cryptool.org/de/cto/vigenere`, um den Text zu entschlüsseln:

- Kopieren Sie den verschlüsselten Text in das Feld „Verschlüsselter Text“.
- Klicken Sie auf den Pfeil zwischen den beiden Textboxen, sodass dieser von „Verschlüsselter Text“ zu „Klartext“ deutet.
- Testen Sie verschiedene Schlüssel. Vorher können Sie die Häufigkeit der Buchstaben im verschlüsselten Text ermitteln. Bedenken Sie aber, dass jeder Buchstabe im Klartext je nach Position zwei verschiedenen Buchstaben im verschlüsselten Text entspricht.

GUH HLSHZHDH OKUIRUQ LEW QLZ HUQRDOK LX YHDNQQPHE YQURDTUQQ, PDE MQ QMFT OMHZJQ GQV EFTOGHEVQOE GQQZROK DHXDFLH VUFTHD LEW. PLQVQ FTLRIDH UVF HUQ NHUVBLQO RXQU QLZH BRXBMOBKMEQWUVOKQ YQUEFTOGHEVQOGQS, GM LY JQJQQEDFC LXD PAQADXSTDNHFLEFTHZ YQUEFTOGHEVQOGQS PQKDHDH HHDVOKUHPHZH MOBKMEQWQ YQUIHZGQW IHDGQQ.

Beispiel 11.4. In diesem Beispiel verschlüsseln wir Texte per Caesar Chiffre wie in Bemerkung 3.4 aus der Vorlesung für $r = 2$: Zuerst fügen wir hinter jeden Buchstaben des ursprünglichen Textes einen weiteren Buchstaben ein. Diese Buchstaben werden per Zufallsgenerator bestimmt. Danach übersetzen wir die Buchstabenpaare in Zahlen:

$$\text{AA} \leftrightarrow 0,\ \text{AB} \leftrightarrow 1, \ldots\ \text{ZZ} \leftrightarrow 675,$$

verschieben alle Zahlen modulo 676 um den Caesar-Schlüssel 314 und übersetzen die Zahlen zurück in Buchstabenpaare.

(a) Verschlüsseln Sie auf diese Art das Wort `CAESAR`.

(b) Ermitteln Sie den Klartext zum verschlüsselten Wort `FIQIJOFQ`.