Aufgabe 1.1 (3 Pkt.)

Betrachten Sie die affinen Verschlüsselungsfunktionen der Form $E(x) = (k_1 x + k_2) \bmod 26$ mit $k_1, k_2 \in \mathbb{Z}_{26}$. ($\mathbb{Z}_{26}$ bezeichne den Restklassenring der ganzen Zahlen modulo 26.) Wir nennen einen Schlüssel (k_1, k_2) *zulässig*, wenn er eine eindeutige Dechiffrierung aller chiffrierten Nachrichten ermöglicht.

Betrachten Sie die Schlüssel $(k_1, k_2) = (11, 13)$ sowie $(k_1, k_2) = (13, 11)$. Geben Sie jeweils die Entschlüsslungsfunktion an, falls es sich um einen zulässigen Schlüssel handelt. Zeigen Sie andernfalls an einem Beispiel, dass der Schlüssel nicht zulässig ist.

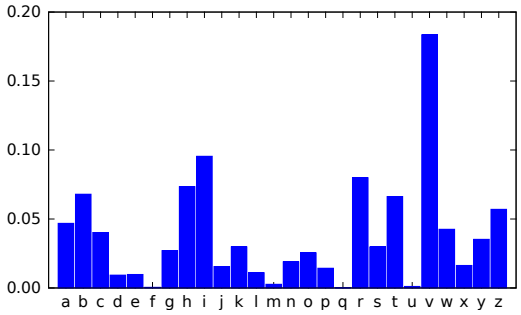
Aufgabe 1.2 (4 Pkt.)

Eine Nachricht werde auf drei Arten verschlüsselt. Es ergeben sich vier Texte:

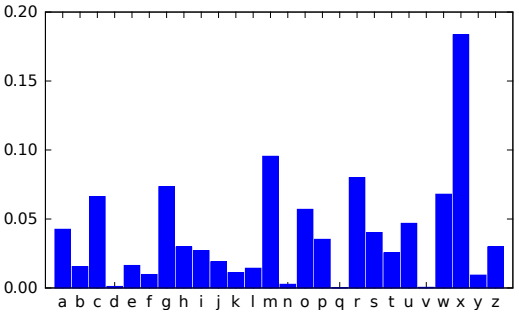
(1) Klartext (in einer Phantasiesprache) (2) Cäsar-Chiffre (3) homophone Chiffre (Buchstaben werden durch die Buchstabenpaare von aa bis zz verschlüsselt) (4) allg. Substitutionschiffre

Die vier Texte besitzen die abgebildeten Buchstabenhäufigkeiten (a) – (d). Ordnen Sie diese Häufigkeiten den Texten (1) – (4) zu, begründen Sie kurz Ihre Wahl. In welchen Fällen ist eine eindeutige Zuordnung unmöglich?

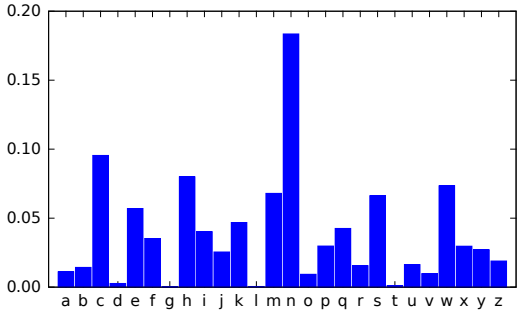
(a)



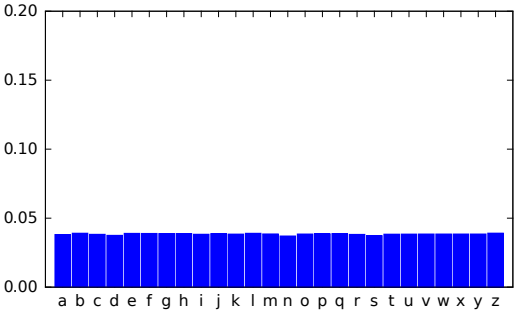
(c)



(b)



(d)



Aufgabe 1.3 (3 Pkt.)

Im rubikon finden Sie eine Cäsar-chiffrierte Datei caesar_shift.txt. Chiffriert wurden ausschließlich die Buchstaben 'a' bis 'z', alle übrigen Zeichen (Satz- und Leerzeichen, Zeilenumbrüche) wurden unverändert übernommen. Geben Sie die Konstante an, um welche die Buchstaben verschoben wurden, sowie den Namen des Gedichts und den Namen des Autors.

Hinweise: Ein Programm, welches die Buchstabenhäufigkeit analysiert, könnte hilfreich sein. Sie finden für deutsche Texte eine Datei Buchstabenhäufigkeiten Deutsch.txt im rubikon.

Aufgabe 1.4 (2 Pkt.)

Eine affin-lineare Blockchiffre über dem Alphabet $R \coloneqq \mathbb{Z}_n$ ist gegeben durch eine invertierbare Matrix $A \in R^{k \times k}$ und einen beliebigen Vektor $b \in R^k$. Zur Verschlüsselung wird die Nachricht erst in Blöcke $m_1, m_2, \ldots$ aus jeweils k aufeinanderfolgenden Zeichen eingeteilt. (Unter Umständen müssen Füllzeichen an die Nachricht angehängt werden, damit deren Länge ein Vielfaches der Blocklänge k wird.) Dann wird jeder Block $m_i \in R^k$ verschlüsselt zu $c_i \coloneqq Am_i + b \in R^k$.

Berechnen Sie die Dekodierfunktion zu folgender affin-linearen Blockchiffre mit Blocklänge $k = 2$, Modul $n = 7$:

$$A = \begin{pmatrix} 3 & 5 \\ 4 & 6 \end{pmatrix} \quad \text{und} \quad b = \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

Aufgabe 1.5 (1+2 Pkt.)

Ein Angreifer hat einen Klartext $m = m_1 \ldots m_n$ und den zugehörigen Chiffretext $E(m) = c = c_1 \ldots c_n$ abgefangen. Außerdem sei das verwendete Verschlüsselungsverfahren bekannt:

a) Cäsar-Chiffre $E(m) = (m + k) \bmod 26$

b) affine Chiffre $E(m) = (k_1 m + k_2) \bmod 26$

Er versucht, daraus den verwendeten Schlüssel zweifelsfrei zu rekonstruieren. Geben Sie jeweils den kleinstmöglichen Wert der Länge n an, bei dem der Angreifer unter Umständen Erfolg hat, und begründen Sie Ihre Antwort. Muss m zusätzliche Bedingungen erfüllen?

Aufgabe 1.6 (1 Pkt.)

Lösen Sie die SPOX-Aufgabe Life, the Universe, and Everything (`http://theoulm.spox.spoj.pl/KRYPT16/units/problem/124/`). Mit dieser Aufgabe sollen Sie sich mit dem SPOX-System vertraut machen.