Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2018/19
19. Okt. 2018

Übungen zur Vorlesung Kryptographie

Blatt 1

Aufgabe 1

Der folgende Geheimtext entstand aus einem deutschen Klartext durch monoalphabetische Substitution mit einem Caesar-Shift $\sigma_t : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad x \mapsto x + t$.

```
CEODY XSECL OCMRB SOLNS OFYXM KOCKB LOXED JDOQO ROSWC MRBSP D
```

Wie lautet der Klartext?

Aufgabe 2

Der folgende Geheimtext entstand aus einem englichen Klartext durch Anwendung einer affin-linearen monoalphabetischen Substitution $\varphi_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad x \mapsto ax + b$, ($a$ teilerfremd zu 26).

```
WQVBD XHLAI NRGCN YEDZU PNKVI WQVST MFONJ
```

Man finde den Klartext und bestimme a, b.

Aufgabe 3

Eine Permutation des Alphabets $\mathfrak{A} = \{\texttt{A},\texttt{B},\ldots,\texttt{Y},\texttt{Z}\}$ kann durch ein Kennwort und einen Offset $\xi \in \mathfrak{A}$ wie folgt definiert werden: Die Buchstaben des Kennwortes werden in der Reihenfolge ihres Auftretens, wobei wiederholt auftretende Buchstaben nur beim ersten Vorkommen verwendet werden, für die Elemente aus $\mathfrak{A}$, beginnend mit dem Offset, substituiert. Ist der Buchstabenvorrat des Kennworts erschöpft, so wird mit den im Kennwort nicht vorkommenden Buchstaben in alphabetischer Reihenfolge fortgefahren (alles zyklisch modulo 26).
Beispielsweise ergibt das Kennwort `WINTERSEMESTER` mit dem Offset `K` die Permutation

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
KLOPQUVXYZWINTERSMABCDFGHJ
```

Der folgende Geheimtext entstand aus einem deutschen Klartext durch Anwendung einer monoalphabetischen Substitution der obigen Art.

```
VWDDP WFEWA ZPXFW XPAAV WEHWD ERZJG BVWBW BSUGD BPAIE FWBSP MPATZ PEZUY YI
```

Man finde den Klartext sowie das Kennwort mit Offset.

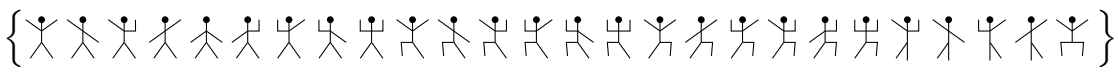
Hinweis. Es werde als bekannt vorausgesetzt, dass der Klartext mit `DER` beginnt.

---

b.w.

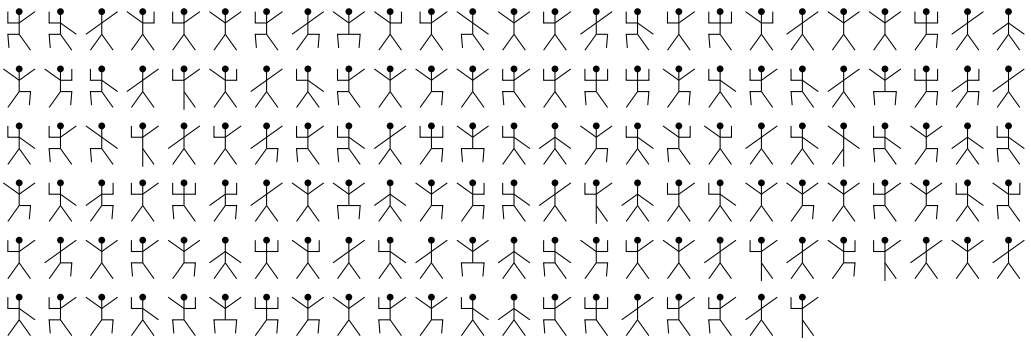
Aufgabe 4

Das folgende Geheimschrift-Alphabet

$\mathfrak{B} :=$ 

einer monoalphabetischen Substitution $\sigma : \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{Z}\} \to \mathfrak{B}$ stammt (in abgewandelter Form) aus einer Kurzgeschichte von Sir Arthur Conan Doyle.

Man entschlüssele den folgenden Geheimtext, der aus einem englischen Klartext mittels einer solchen Substitution entstand.



Hinweise

a) Das häufigste Trigramm im Englischen ist `THE`.

b) Der Klartext enthält das Wort `HOLMES`.