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

SS 2009
17. Juni 2009

Algorithmische Zahlentheorie

Übungsblatt 9

Aufgabe 33

a) Welchen Bedingungen müssen die Zahlen $(a, b) \in \mathbb{Z}^2$ genügen, damit die Abbildung

$$\phi_{ab} : \mathbb{Z}/26 \longrightarrow \mathbb{Z}/26, \qquad x \mapsto (ax + b) \bmod 26,$$

bijektiv ist? Die Menge aller solcher bijektiven Abbildungen werde mit $\mathrm{Aff}(1, \mathbb{Z}/26)$ bezeichnet.

b) Eine bijektive Abbildung $\phi : X \to X$ heißt Involution, wenn $\phi \circ \phi = \mathrm{id}_X$, aber $\phi \neq \mathrm{id}_X$. Man bestimme alle Involutionen $\phi_{ab} \in \mathrm{Aff}(1, \mathbb{Z}/26)$.

Aufgabe 34

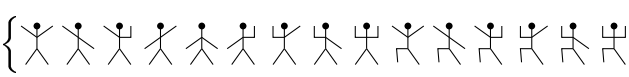
Der folgende Geheimtext entstand mit einer monoalphabetischen Substitution $\phi_{ab} \in \mathrm{Aff}(1, \mathbb{Z}/26)$ aus einem deutschen Klartext $x \in (\mathbb{Z}/26)^{50}$ (mit der Identifizierung $\{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \mathrel{\widehat{=}} \mathbb{Z}/26$):

```
UOROE XLJEB SZGCY JSYJG PPFGS FWRMS RCGRV XSGYJ ZHWAR EYASR
```

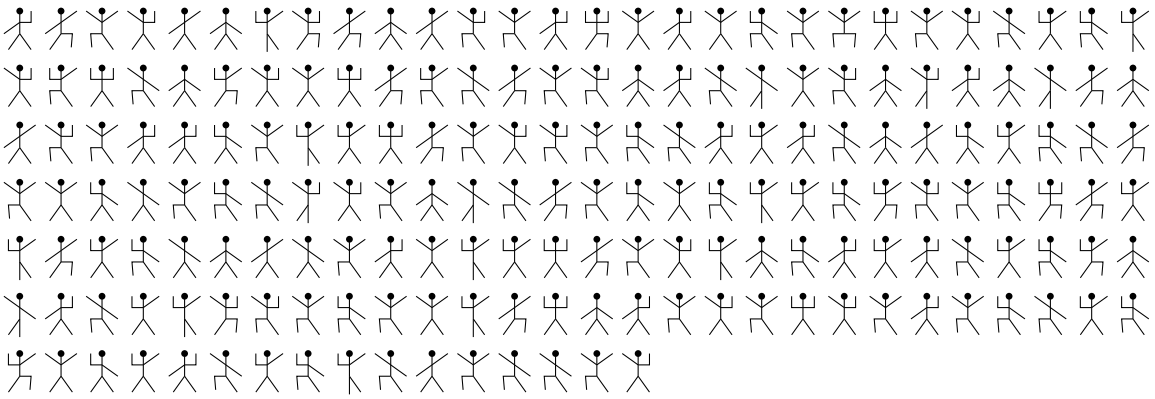
Man bestimme den Klartext und die Parameter a, b.

Aufgabe 35

Eine monoalphabetische Substitution $\pi : \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{Z}\} \to \mathfrak{B}$, wobei

$\mathfrak{B} =$  ,

wurde auf einen englischen Klartext angewendet. Der entstandende Geheimtext lautet:



Man rekonstruiere den Klartext und, soweit möglich, die Abbildung π.

---

b.w.

Aufgabe 36

Ein Pseudo-One-Time-Pad

$$(z_0, z_1, \ldots, z_{43}) \in (\mathbb{Z}/256)^{44}$$

wurde durch eine zweigliedrige Rekursion

$$z_k := (a \cdot z_{k-1} + b \cdot z_{k-2}) \bmod 256$$

erzeugt. Dieser Byte-Vektor wurde durch bitweises `XOR` mit einem ASCII-Klartext der Länge 44 verknüpft. Der entstehende Byte-Vektor lautet (in hexadezimaler Schreibweise)

```
8EEC 02DA 883B 0462 4317 1789 A81C AA50 9EC1 EE8D 2B02 7689 B454 157A
667A 66BD CEEB 6EA0 C36C BEB3 2650 9AB4
```

Der Klartext beginnt mit den vier Zeichen '`Die `', hexadezimal `4469 6520`. Man berechne z_0, z_1, a, b und den gesamten Klartext.

Abgabetermin: Freitag, 26. Juni 2009, 14 Uhr, Übungskasten im 1. Stock