Übungsblatt 2

Kryptographie und Kodierungstheorie
WiSe 16/17

Aufgabe 2.1. Sei p eine Primzahl. Bestimmen Sie die Ordnung der Gruppe

$$\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in (\mathbb{Z}/p\mathbb{Z})^{2\times 2} \mid (ad - bc) \in (\mathbb{Z}/p\mathbb{Z})^* \right\}.$$

Aufgabe 2.2. Sie fangen die Nachricht

NIMYKCYVKHVRPRBHWJPIBCSLLMQBRBMISLV

ab und wollen diese entschlüsseln. Ihnen ist bekannt, dass die Vigenère-Chiffre mit Blocklänge 3 benutzt wurde. Außerdem wissen Sie, dass der Klartext von der Form *AutorTiteldesbuches* ist, wobei man Ihnen mitgeteilt hat, dass der Anfangsbuchstabe des Vornamens des Autors G ist.
Nur lesen, wenn Sie nicht weiterkommen:
Wenn Sie keinen Computer benutzen möchten, dann dürfen Sie benutzen, dass der Vorname gerge lautet.

Aufgabe 2.3. Eine Botschaft ist mit der Hill-Chiffre verschlüsselt worden, der Schlüsseltext ist

KARCAOXWGCYWXXRC

Wie lautet der zugehörige Klartext?
Hinweis: Wenn Sie den Text

WARUMSINDWIRHIER

auf die selbe Art und Weise verschlüsseln, dann erhalten Sie den Schlüsseltext

WYZPOGVERVHEFXDC.