Kryptographie *WS 2015/16*
Barbara Baumeister
Tutoren: Apolonia Gottwald, Soeren Senkovic

1. Übungsblatt

Abgabe: Donnerstag, 29.10.2015

Aufgabe 1 Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, e, d)$ mit $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n^r, \mathcal{K} = S_r$ und für $\pi \in S_r$ sei

$$e_\pi(x_1, \ldots, x_r) = (x_{\pi(1)}, \ldots, x_{\pi(r)})$$

auch genannt Permutationschiffre. Zeigen Sie, dass diese linear ist (d.h. das alle Verschlüsselungsfunktionen linear sind).

Aufgabe 2 Zeigen Sie: Die Matrix in $\mathbb{Z}_n^{r \times r}$ ist invertierbar über $\mathbb{Z}_n$ genau dann, wenn $\det(A)$ invertierbar ist in $(\mathbb{Z}_n \setminus \{0\}, \cdot)$.

Aufgabe 3 KIELSGLMENWXYSYOWPHWJFJWLRBBFXPRVOSVOX
FIFXZGYMSYKIELSGLMEIWKGSYOWEPISFVXUOROEB

Entschlüsseln Sie diesen Text, der mit der Vignere-Chiffre verschlüsselt wurde. Welcher Schlüssel wurde verwendet?

Aufgabe 4 Beschreiben Sie eine Attacke mit gewähltem Klartext auf die affin lineare Chiffre mit möglichst wenig gewählten Klartexten.