1. Übungsblatt

Abgabe: Mittwoch, 6.5.09

Aufgabe 1 Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, e, d)$ mit $\mathcal{P} = \mathcal{C} = Z_n^r$ die Permutationschiffre. Zeigen Sie, dass sie linear ist (d.h. dass alle Verschlüsselungsfunkionen linear sind).

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

Aufgabe 3 Beschreiben Sie eine Attacke mit gewähltem Klartext auf die affin lineare Chiffre mit möglichst wenig gewählten Klartexten.

Aufgabe 4 Ist die Primfaktorzerlegung von $m = p_1^{k_1} \cdots p_r^{k_r}$ bekannt, so lässt sich $\varphi(m)$ in $\mathcal{O}(?)$ berechnen. Bestimmen Sie die Laufzeit.