Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 11.07.2005, 14h

Kryptografie
Übungsblatt 12

Aufgabe 33:
Sei $q = 2$, $\mathbb{K} = \mathbb{F}_{q^4}$.

a) Konstruieren Sie den öffentlichen Schlüssel des kleinen Drachen mit den folgenden Daten (Bezeichnungen wie in der Vorlesung): $h = 11$, $\mathbb{K}$ sei präsentiert durch $\mathbb{K} = \mathbb{F}_2[z]/(z^4 + z + 1)$, die Basis $(\beta_1, \ldots, \beta_4)$ gegeben durch $(1, \bar{z}, \bar{z}^2, \bar{z}^3)$, $\mathcal{A} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$, $\mathcal{B} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Ergebnis (ohne Gewähr):

$$
\begin{aligned}
x_3y_3 + x_4y_2 + x_3y_1 + x_1y_2 + x_4y_1 + x_2y_4 &= x_1x_3 + x_3x_4 + x_3x_2 + x_4x_2 + x_2^2 \\
x_1y_1 + x_2y_3 + x_3y_2 + x_4y_4 + x_1y_3 + x_3y_4 + x_1y_2 &= x_3x_4 + x_1x_2 + x_2^2 + x_3^2 \\
x_2y_1 + x_1y_2 + x_4y_3 + x_4y_4 + x_3y_1 + x_1y_4 + x_3y_4 &= x_3x_4 + x_1x_4 + x_4^2 + x_1^2 + x_3x_2 + x_2^2 \\
x_1y_1 + x_4y_4 + x_4y_1 + x_2y_2 + x_2y_4 + x_1y_4 + x_4y_3 + x_2y_3 + x_3y_2 &= \\
& x_3^2 + x_4^2 + x_1x_4 + x_1x_3 + x_3x_2 + x_2^2 + x_1^2 + x_4x_2
\end{aligned}
$$

b) Verschlüsseln Sie den Klartext $(1, 0, 1, 0)$.

c) Entschlüsseln Sie den Geheimtext aus b).