Übungen zur Kryptologie 1 Wintersemester 2003-2004

Johannes Köbler/Lorenz Weizsäcker

Übungsblatt 4

Aufgabe 15

Ein lineares Schieberegister (LSR) der Länge m ist eine Anordnung von m Speicherzellen $k_1, \ldots, k_m$, wobei jede Zelle k_i ein Bit Information speichern kann.

Seien $c_0, \ldots, c_{m-1} \in \{0,1\}$ Konstanten, wobei $c_0 = 1$. Ein Rechenschritt eines LSR besteht darin, zunächst das Bit $\ell = \bigoplus_{j=0}^{m-1} c_j \cdot k_{j+1}$ zu berechnen. Dann wird k_1 ausgegeben und der Inhalt der Speicherzellen um eine Position nach links verschoben, wobei k_m den Wert ℓ erhält. Auf diese Art entsteht eine Bitfolge z_i mit $z_i = k_i$, $1 \leq i \leq m$, und

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \bmod 2, \ i \geq 1.$$

Offensichtlich ist diese Folge nicht zufällig, sondern besteht aus einem sich ständig wiederholenden Muster, dessen Länge als Periode des LSR bezeichnet wird.

a) Konstruieren Sie ein LSR der Länge $m = 5$ mit Periode 31.

b) Zeigen Sie, dass die Periode höchstens $2^m - 1$ ist.

c) Überlegen Sie sich, wie die auf einem LSR basierende Stromchiffre bei Kenntnis von $2m$ aufeinanderfolgenden Klartext/Kryptotext-Bitpaaren gebrochen werden kann, falls $k = (k_1, \ldots, k_m, c_0, \ldots, c_{m-1})$ als Schlüssel benutzt wird.

Aufgabe 16

Entschlüsseln Sie durch eine Häufigkeitsanalyse (von Bigrammen) folgende Kryptotexte.

a) `hssit oient thehs aotre tsehf rteet` (*Hinweis:* Der Klartext wurde durch eine Blocktransposition, mit der Blocklänge 5 verschlüsselt.)

b) `royeg rholr evrvn vgrhe tnkre aacat` (*Hinweis:* Der Klartext wurde durch eine Matrixtransposition mit einer 6×5 Matrix verschlüsselt.)

Aufgabe 17 (schriftlich, 10 Punkte)

a) Durch eine Häufigkeitsanalyse wurde festgestellt, dass eine affine Chiffre `E` auf `l` und `T` auf `g` abbildet. Bestimmen Sie den Schlüssel.

b) Wie Teilaufgabe a, nur wurde `J` auf `t` und `N` auf `v` abgebildet.