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

3. Übungsblatt

Abgabe: Donnerstag, 12.11.2015

Aufgabe 1 (a) Ist die Cäsarchiffre perfekt sicher?

(b) Gegeben sei ein Kryptosystem mit $\mathcal{P} = \{a, b\}, \mathcal{C} = \{A, B\}, \mathcal{K} = \{0, 1\}$ und Verschlüsselungsfunktionen e_0 und e_1 mit $e_0(a) = A, e_0(b) = B$, $e_1(a) = B$ und $e_1(b) = A$. Weiter sei auf $\mathcal{P}$ ein Wahrscheinlichkeitsmaß durch $P(a) = 1/3$ und $P(b) = 2/3$ definiert.
Gibt es ein Wahrscheinlichkeitsmaß auf $\mathcal{K}$ so, dass dieses Kryptosystem perfekt sicher ist?

Aufgabe 2 Betrachte die lineare Blockchiffre mit Blocklänge n über dem Alphabet $\mathcal{A} = \mathbb{F}_q$, q eine Primzahlpotenz. Dabei sei sowohl auf dem Klartextraum $\mathcal{P} = \mathcal{A}^n$ als auch auf dem Schlüsselraum $\mathcal{K}$ der invertierbaren $n \times n$-Matrizen über $\mathbb{F}_q$ die Gleichverteilung gegeben.

(a) Ist die Blockchiffre perfekt sicher?

(b) Ändert sich daran etwas, wenn man sowohl im Klar- als auch im Chiffretextraum die 0 entfernt?

Aufgabe 3 Sei $K = \mathbb{F}_{2^n}$ und $a \in K$. Hat die Gleichung $x^2 + x = a$ eine Lösung in K, so gilt $a + a^2 + \cdots + a^{2^{n-1}} = 0$.
Hinweise: In K gilt $x^{2^n} = x$. Betrachten Sie $x^2 + x = a, x^4 + x^2 = a^2$ usw.

Aufgabe 4 Sei $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ eine invertierbare Abbildung und $k \in \mathbb{F}_{2^n}$ ein Schlüssel mit dem wir eine Nachricht $x \in \mathbb{F}_{2^n}$ zu $f(x + k)$ verschlüsseln. Setze $N_f = |\{f(x + k) + f(x) \mid x \in \mathbb{F}_{2^n}\}|$. Zeigen Sie:

(a) $N_f \leq 2^{n-1}$.

(b) Eine Funktion heisst APN (Almost Perfect Nonlinear), falls $N_f = 2^{n-1}$ ist. Zeigen Sie, dass für n ungerade

$$f(x) = \begin{array}{ll} x^{-1}, & \text{falls } x \neq 0 \\ 0, & \text{falls } x = 0 \end{array}$$

eine APN-Funktion ist.
Hinweis: Es gilt $f(x) = x^{2^n-2}$. Zeigen Sie, dass $f(x+k)+f(x) = b$ für alle $b \in \mathbb{F}_{2^n}$ und $k \in \mathbb{F}_{2^n}$, $k \neq 0$ keine oder genau 2 Lösungen hat. Wir dürfen $k = 1$ annehmen. Sind $x \neq 0, x+1 \neq 0$ Lösungen, so sind es die einzigen. Untersuchen Sie nun den Fall, dass $x = 0$ und $x = 1$ Lösungen sind, und benutzen Sie Aufgabe 3.