Kryptographie *WS 2012/13*
Barbara Baumeister

3./4. Übungsblatt

Abgabe: Donnerstag, 8.11.2012

Aufgabe 1 Sei $n > 1$, $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Zeigen Sie, dass $\overline{a} \in \mathbb{Z}_n^*$ genau dann gilt, wenn $\mathrm{ggT}(a, n) = 1$ ist.

Aufgabe 2 Geben Sie eine Permutation von $\mathbb{F}_2^n$ an, die nicht affin linear ist.

Aufgabe 3 Zeigen Sie, dass auf folgende Weise ein Kryptosystem definiert ist.
Sei w ein Wort über $\{A, B, \ldots, Z\}$. Wähle zwei Schlüssel k_1 und k_2 für die Cäsarchiffre. Verschlüssele Zeichen mit ungeradem Index unter Verwendung von k_1 und die mit geradem Index unter Verwendung von k_2. Dann kehre die Reihenfolge der Zeichen um.
Bestimmen Sie den Klartextraum, den Schlüsselraum und den Chiffretextraum.

Aufgabe 4 Seien $a, b \in \mathbb{N}$ mit $a \geq b$. Wir berechnen mit dem euklidischen Algorithmus $\mathrm{ggT}(a, b)$. Wir wissen, dass die Anzahl der Iterationen n durch eine Funktion, die $\mathcal{O}(l(a))$ ist, nach oben abgeschätzt werden kann.

(a) Zeigen Sie, $\prod_{k=1}^{n} q_k \leq a$.

(b) Zeigen Sie, dass der k-te Schritt in dem euklidischen Algorithmus die Laufzeit $\mathcal{O}(l(b)(log_2(q_k) + 1))$ hat.

(c) Zeigen Sie, das der euklidische Algorithmus die Laufzeit $\mathcal{O}(l(a)l(b))$ hat.

Aufgabe 5 Seien $a, b \in \mathbb{F}_{2^8}$ in binärer Form $a = (00000010)$ und $b = (00000011) = a + 1$.

(a) Zeigen Sie, dass die Matrix

$$T = \begin{pmatrix} a & b & 1 & 1 \\ 1 & a & b & 1 \\ 1 & 1 & a & 1 \\ b & 1 & 1 & a \end{pmatrix} \in Mat_{4,4}(\mathbb{F}_{2^8}).$$

invertierbar ist

(b) Bestimmen Sie mit einem Computeralgebrasystem T^{-1}.

Aufgabe 6 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 7 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 6.