Kryptographie *WS 2012/13*
Barbara Baumeister

2. Übungsblatt

Abgabe: Donnerstag, 25.11.2012

Aufgabe 1 Betrachte Sie die linerare Blockchiffre der Länge n über dem Alphabet $\mathcal{A} = \mathbb{F}_q$, q eine Primzahlpotenz. Auf dem Klartextraum als auch dem Schlüsselraum der über $\mathbb{F}_q$ invertierbaren $n \times n$-Matrizen sei die Gleichverteilung gegeben.

(a) Ist die Blockchiffre perfekt sicher?

(b) Ändert sich daran etwas, wenn die 0 sowohl aus dem Klar- als auch dem Chiffretextraum entfernt wird?

Aufgabe 2 Gegeben sei eine affin linerare Blockchiffre der Länge r über $\mathbb{Z}_m$. Es wird mit dem geheimen Schlüssel (A, b) verschlüsselt. Wir wollen den Schlüssel mit Hilfe des Angriffs mit bekanntem Klartext herausfinden.

(a) Gegeben seien $r+1$ Vektoren $v_0, \ldots, v_r \in \mathbb{Z}_m^r$ und ihre Verschlüsselungen $c_0, \ldots c_r$. Weiter sei $\mathrm{ggT}(\det(v_1 - v_0, \ldots, v_r - v_0), m) = 1$. Zeigen Sie, dass dann A und b bestimmt werden können.

(b) Ist es möglich den Schlüssel herauszufinden, wenn nur für r Vektoren $v_1, \ldots, v_r \in \mathbb{Z}_m^r$ die Verschlüsselungen $c_1, \ldots c_r$ bekannt sind?

Aufgabe 3 (a) Gegeben sind zwei natürliche Zahlen a und b in binärer Darstellung. Führen Sie die Subtraktion $a - b$ auf eine Addition zurück.
(Hinweis: Rechnen Sie modulo 2^n, wobei $n = \max(l(a), l(b)) + 1$ ist, und betrachten Sie zu b das Element $\overline{b}$, $0 \leq \overline{b} \leq 2^n - 1$, welches durch $b + \overline{b} = 2^n - 1$ gegeben ist.)

(b) Führen Sie das Verfahren an den Zahlenpaaren $(a, b) = (43, 17)$ und $(a, b) = (35, 67)$ durch.

Aufgabe 4 Entschlüsseln Sie den folgenden mit Vignère verschlüsselten Text:

FSUQQDVZQBIVCSXPGWQPWBGIPKDVGWQIUHDKU
JHVUQKAWBGIPGLIRTOIIHHQWGVQCBZMUGHRVOJEGUOMEVLLPNXOWSVWGB