Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 20.11.2014
Abgabe: Mo. 30.11.2014 bis 14:00 (D3 Kasten)/14:45 Uhr (Fürstenallee)

Einführung in Kryptographie

WS 2015/2016

Heimübungszettel 3

AUFGABE 1 (6 Punkte)**:**
Sei Q eine beliebige Wahrscheinlichkeitsverteilung auf $\mathbb{Z}_{26}^* = \{x \in \mathbb{Z}_{26} : x \text{ ist teilerfremd zu } 26\}$. Zeigen Sie, dass die *affin-lineare* Verallgemeinerung der Caesar-Chiffre aus Heimübung 1 perfekt geheim ist, wenn jeder Schlüssel $(a, b) \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$ mit der Wahrscheinlichkeit $Q(a)/26$ gewählt wird. Es wird also a nach einer beliebigen aber festen Verteilung und b zufällig gleichverteilt gezogen.

AUFGABE 2 (6 Punkte)**:**
In der Vorlesung wurde mittels des Satzes von Shannon gezeigt, dass das One-Time-Pad perfekt geheim ist, solange $\Pr(p) > 0$ für alle $p \in \mathcal{P}$ gilt. Allerdings bedeutet die Wahl des Schlüssels $k = 0^n$, dass ein Klartext $m \in \{0,1\}^n$ unverändert gesendet wird, denn

$$E_{0^n}(m) = m \oplus 0^n = m \ .$$

a) Ihr Tutor schlägt Ihnen daher folgende Verbesserung des One-Time-Pads vor: Als Schlüssel wird zufällig gleichverteilt ein Element aus $\{0,1\}^n \setminus \{0^n\}$ gewählt. Das restliche Verfahren bleibt wie in der Vorlesung beschrieben. Ist das vorgeschlagene Verfahren noch immer perfekt geheim? Beweisen Sie Ihre Antwort!

b) Zeigen Sie, dass die Einschränkung $\Pr(p) > 0$ für alle $p \in \mathcal{P}$ nicht notwendig ist. Zeigen Sie also, dass das One-Time-Pad unabhängig von der Verteilung auf dem Nachrichtenraum perfekt geheim ist.

AUFGABE 3 (6 Punkte)**:**
Gegeben sei eine beliebige *Feistel-Chiffre* mit Blocklänge $n = 2t$, Funktion $f : \{0,1\}^l \times \{0,1\}^t \to \{0,1\}^t$ und Rundenanzahl r. Sei c der Chiffretext, der durch Verschlüsselung einer Nachricht m mit den Rundenschlüsseln $k_1, k_2, \ldots, k_r$ entsteht. Zeigen Sie, dass dann die Verschlüsselung von c mit Rundenschlüsseln $k_r, k_{r-1}, \ldots, k_1$ in umgekehrter Reihenfolge die Nachricht m ergibt.

AUFGABE 4 (8 Punkte)**:**
Wir betrachten die erste Runde der DES Verschlüsselung.

a) Verschlüsseln Sie $m_1 = 0^{64}$ und $m_2 = 0^{60}1000$ aus $\mathcal{P} = \{0,1\}^{64}$ mit DES und dem Rundenschlüssel $k_1 = (01)^{24}$. Ersetzen Sie dabei der Einfachheit halber die S-Boxen $S_2, \ldots, S_8$ jeweils durch S_1 aus der Vorlesung.

b) Zeigen Sie, dass Lemma 4.1 und Lemma 4.2 aus der Vorlesung für m_1 und m_2 aus diesem Beispiel erfüllt sind.

c) An wievielen Stellen unterscheiden sich die Ausgaben L_1, R_1 für die beiden Eingaben m_1 und m_2?