Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 15.1.2016

Einführung in Kryptographie

WS 2015/2016

Präsenzübungszettel 6

AUFGABE 1:
Betrachten Sie das Elgamal-Krytosystem. Es sei $sk = (p, g, a)$ mit $p = 7$, $g = 3$ und $a = 4$.

a) Zeigen Sie, dass (p, g, a) den Anforderungen genügt, die an einen geheimen Schlüssel für das Elgamal-Kryptosystem gestellt werden.

b) Bilden Sie den dazu gehörenden öffentlichen Schlüssel.

c) Verschlüsseln Sie die Nachricht $m = 3$ mit der Zufallszahl $r = 2$.

d) Entschlüsseln Sie den Chriffretext $(c_1, c_2) = (6, 4)$.

AUFGABE 2:

a) Geben Sie eine zyklische Gruppe G der Größe $n \in \mathbb{N}$ an, in der das Diskrete Logarithmus Problem leicht zu lösen ist.

b) Zeigen Sie, dass das Diskrete Logarithmus Problem in G wirklich einfach zu lösen ist. Definieren Sie dazu einen Algorithmus, der $\text{dlog}_g(a)$ für *beliebige* Generatoren $g \in G$ mit G aus a) in Zeit $\mathcal{O}(\log(n)^c)$, (c konstant) berechnen kann. Erklären Sie auch, warum Ihr Algorithmus korrekt ist und die geforderte Laufzeit besitzt.

AUFGABE 3:
Zeigen Sie: Nicht jede kollisionsresistente Funktion ist eine Einwegfunktion!
Tipp: Suchen Sie ein einfaches Beispiel und beachten Sie, dass hier nicht nur Hashfunktionen und Kompressionsfunktionen betrachtet werden.

AUFGABE 4:
Gegeben seien zwei Hashfunktionen $h_1 : \{0,1\}^* \to \{0,1\}^n$ und $h_2 : \{0,1\}^* \to \{0,1\}^n$, von denen mindestens eine kollisionsresistent ist. Zeigen Sie, dass dann auch die Hashfunktion $g : \{0,1\}^* \to \{0,1\}^{2n}$ mit $g(x) = h_1(x) \| h_2(x)$ kollisionsresistent ist. Hier bezeichne $\|$ die Konkatenation in $\{0,1\}^*$.