Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Felix Heuer

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2011

Blatt 1 / 13. und 15. April 2011

Definition 1. Sei G eine endliche (multiplikative) Gruppe und $g \in G$. Die *Ordnung von* g ist definiert als

$$\mathrm{ord}(g) := \min\{i \in \mathbb{N} : g^i = 1\} \ .$$

Eine Gruppe heißt *zyklisch*, falls es einen *Generator* $g \in G$ gibt, d.h. wir können G darstellen als

$$G = \{1, g, g^2, \ldots, g^{\mathrm{ord}(g)-1}\} \ .$$

AUFGABE 1. Algebraisches.
Sei G eine endliche Gruppe mit $|G| = n$ und sei $g \in G$ ein Element der Ordnung $i = \mathrm{ord}(g)$. Zeigen Sie:

a) $g^k = 1 \Leftrightarrow i|k$ (insbesondere folgt $i|n$)

b) $g^x = g^y \Leftrightarrow x \equiv y \bmod i$

c) Wenn n prim ist, dann ist G zyklisch.

AUFGABE 2. Schlamüssel.
Betrachten Sie das folgende Schlüsselaustausch Protokoll:

1. Alice wählt zufällig $k, r \xleftarrow{R} \{0,1\}^n$ und sendet $s := k \oplus r$ an Bob.
2. Bob wählt zufällig $t \xleftarrow{R} \{0,1\}^n$ und sendet $u := s \oplus t$ an Alice.
3. Alice berechnet $w := u \oplus r$ und sendet w an Bob.
4. Alice gibt den Schlüssel k aus und Bob berechnet den Schlüssel als $w \oplus t$.

Zeigen Sie, dass Alice und Bob denselben Schlüssel berechnen. Analysieren Sie die Sicherheit des Protokolls, d.h. beweisen Sie entweder die Sicherheit oder geben Sie einen konkreten Angriff an.

AUFGABE 3. Reduktion.
Sei $\mathcal{G}$ ein ppt-Algorithmus, der zur Eingabe 1^n eine zyklische Gruppe G der Ordnung q und einen Generator g erzeugt wobei q Bitlänge n hat. Wir schreiben kurz $(G, g, q) \leftarrow \mathcal{G}(1^n)$.

Zeigen Sie: Wenn DDH hart ist bzgl. $\mathcal{G}$, so ist auch CDH hart bzgl. $\mathcal{G}$.

Beachten Sie hierbei, dass der Wahrscheinlichkeitsraum in den jeweiligen Definitionen (siehe Folie 16 und 17) über die zufällige Wahl der Exponenten $x, y, z \in_R \mathbb{Z}_q$ sowie die Münzwürfe von $\mathcal{A}$ und $\mathcal{G}$ gebildet wird.

AUFGABE 4. Null Problemo. (5 Punkte)
Betrachten Sie das folgende Problem:

> Sei p eine Primzahl und $x \in \mathbb{Z}_{p-1}^*$.
> Gegeben p, x und $y := g^x \bmod p$
> wobei g ein zufälliger Wert zwischen 1 und $p-1$ ist.
> Finde g, d.h. berechne $y^{\frac{1}{x}} \bmod p$.

Konstruieren Sie einen effizienten Algorithmus für das obige Problem. Verifizieren Sie seine Korrektheit und analysieren Sie die Laufzeit.

Hinweis: Bei der Analyse der Laufzeit dürfen Sie benutzen, dass das Berechnen von Inversen in $\mathbb{Z}_{p-1}^*$ effizient in Laufzeit $\mathcal{O}(\log_2(p-1)^2)$ möglich ist (mittels erweitertem Euklidischen Algorithmus).