Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 10 / 16./17. Dezember 2013

AUFGABE 1:

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 $(g, q) \leftarrow \mathcal{G}(1^n)$.

Beweisen Sie folgende Aussagen:

(a) Wenn das DDH-Problem hart ist bzgl. $\mathcal{G}$, so ist auch das CDH-Problem hart bzgl. $\mathcal{G}$.

(b) Wenn das CDH-Problem hart ist bzgl. $\mathcal{G}$, so ist auch das DL-Problem hart bzgl. $\mathcal{G}$.

AUFGABE 2:

Betrachten Sie das folgende Schlüsselaustauschprotokoll:

1) Alice wählt $k, r \in_R \{0,1\}^n$ und sendet $s := k \oplus r$ an Bob.
2) Bob wählt $t \in_R \{0,1\}^n$ 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 $w \oplus t$.

(a) Zeigen Sie, dass Alice und Bob denselben Schlüssel berechnen.

(b) Analysieren Sie die Sicherheit des Protokolls, d.h. beweisen Sie entweder die Sicherheit oder geben Sie einen konkreten Angriff an.

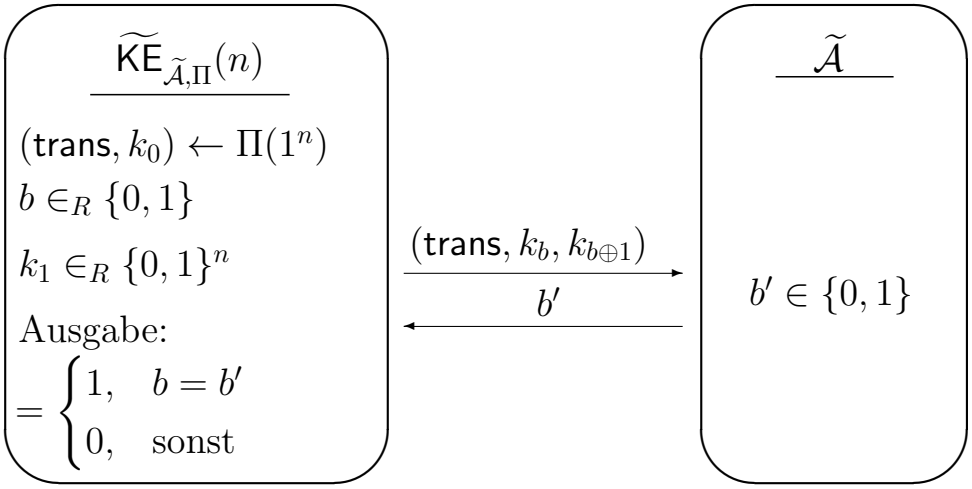
Bitte wenden!

AUFGABE 3:

Definition: Ein Schlüsselaustauschprotokoll Π heißt *stark sicher* gegen passive Angriffe, falls für alle ppt-Angreifer $\widetilde{A}$ gilt, dass

$$\mathsf{Ws}[\widetilde{\mathsf{KE}}_{\widetilde{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n).$$

Diese Definition betrachtet eine Modifikation $\widetilde{\mathsf{KE}}$ des KE-Spiels aus der Vorlesung. Der Angreifer $\widetilde{\mathcal{A}}$ erhält die Challenge $(\mathsf{trans}, k_b, k_{b\oplus 1})$ anstelle von (trans, k_b), d.h. $\widetilde{\mathcal{A}}$ bekommt den korrekt erzeugten *und* den zufällig gewählten Schlüssel als Eingabe und muss entscheiden, in welcher Reihenfolge er diese erhalten hat.



Zeigen Sie: Jedes *stark sichere* Schlüsselaustauschprotokoll Π ist *sicher*.

AUFGABE 4:

Beurteilen Sie, ob das folgende Problem schwer ist.

Gegeben sei eine Primzahl p, ein Wert $x \in \mathbb{Z}_{p-1}^*$ und $y := g^x \pmod p$, wobei $g \in_R \{1, 2, \ldots, p-1\}$. Gesucht ist g, das heißt es soll $y^{\frac{1}{x}} \pmod p$ berechnet werden.

Halten Sie das Problem für schwer, dann zeigen Sie eine Reduktion auf eines der in der Vorlesung behandelten schweren Probleme. Glauben Sie hingegen, das Problem sei einfach, dann geben Sie einen Algorithmus zur Lösung des Problems an, zeigen dessen Korrektheit und analysieren Sie dessen Laufzeit.