

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 11 / 22. Dezember 2010

**AUFGABE 1:**

Konstruieren Sie im Random-Oracle Modell einen  $(\epsilon, q)$ -Algorithmus für das Zweite-Urbild Problem mit

$$\epsilon = 1 - \left(1 - \frac{1}{|\mathcal{Y}|}\right)^{q-1}.$$

**AUFGABE 2:**

Bringen Sie das **Urbild Problem**, das **Zweites-Urbild Problem** und das Problem **Kollision** in Zusammenhang.

Zeigen Sie dazu alle beweisbaren Aussagen der Form "Wenn ich Problem A lösen kann, dann kann ich auch Problem B lösen."

*Bemerkung:* Das bedeutet dann, dass sich Problem B auf Problem A reduzieren lässt,  $B \leq A$ .

**AUFGABE 3:**

Geben Sie einen polynomiellen Algorithmus für das  $k$ -Listenproblem für den Fall  $k \geq n$  über  $\mathbb{F}_{2^n}$  an.

*Hinweis:* Sie können annehmen, dass jede der Listen nur 2 Elemente besitzt. Schon in diesem Fall erwarten Sie eine Lösung.