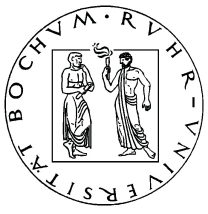
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Alexander Meurer



Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 8 / 03. Februar 2010

AUFGABE 1:
Konstruieren Sie im Random-Oracle Modell einen (ϵ, 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, $B \leq A$.