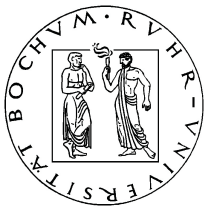
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen, Alexander Meurer



Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 7 / 17.Juli 2008

AUFGABE 1:
Berechnen Sie mit Hilfe des Index-Kalkulus Algorithmus den diskreten Logarithmus $\log_5(14)$ in $\mathbb{Z}_{23}^*$. Verwenden Sie dabei die Faktorbasis $F_3 = \{-1, 2, 3\}$ und die Wahl $r_i = i, i \geq 0$. Geben Sie die diskreten Logarithmen aller Elemente aus F_3 zur Basis 5 in $\mathbb{Z}_{23}^*$ an.

AUFGABE 2:

(a) Seien $v_1, \ldots, v_j \in \mathbb{F}_2^n$ linear unabhängig. Dann ist die Wahrscheinlichkeit, dass ein zufällig aus $\mathbb{F}_2^n$ gezogener Vektor zu $v_1, \ldots, v_j$ linear unabhängig ist, durch $1 - 2^{j-n}$ gegeben.

(b) Seien $v_1, \ldots, v_k \in \mathbb{F}_2^n, k \leq n$ zufällig gewählte Vektoren. Zeigen Sie, dass diese Vektoren mit Wahrscheinlichkeit

$$\prod_{i=0}^{k-1}(1 - 2^{i-n})$$

linear unabhängig sind.

AUFGABE 3:
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 4:
Konstruieren Sie im Random-Oracle Modell einen (ϵ, q)-Algorithmus für das Zweite-Urbild Problem mit

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