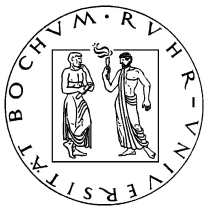
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen, Alexander Meurer



Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 3 / 23. Mai 2008

AUFGABE 1:
(Wiederholung von Übungsblatt 2)
Wir betrachten das DL-Problem: Sei $\beta = \alpha^a \in Z_p^*$, wobei $n = \text{ord}(\alpha)$ gegeben ist und a ermittelt werden soll. Beschreiben Sie einen Meet-in-the-Middle Angriff auf a mit Zeit und Platz $\tilde{\mathcal{O}}(\sqrt{n})$.
Verwenden Sie Ihren Algorithmus, um $\log_5(10)$ in $\mathbb{Z}_{17}^*$ zu berechnen.

AUFGABE 2:
In Pollards Rho-Methode habe das Anfangsstück Länge i und der Kreis Länge $j - i$. Zeigen Sie, dass sich die beiden Känguruhs im Punkt $s_m = s_{2m}$ treffen, wobei

$$m = (j - i) \cdot \left\lceil \frac{i}{j - i} \right\rceil .$$

AUFGABE 3:
Überlegen Sie sich einfache Gegenmaßnahmen gegen Kochers Timing Angriff. Welche Vor- bzw. Nachteile haben Ihre Gegenmaßnahmen?

AUFGABE 4:
Überlegen Sie sich einen einfachen Test, den man nach der Berechnung des Wertes $y = \text{sig}_k(x)$ durchführen kann, um den Bellcore Angriff zu verhindern. Was ist der Nachteil eines solchen Tests?

AUFGABE 5:
Geben Sie unimodulare Transformations-Matrizen für eine Basismatrix $B \in \mathbb{Z}^{3\times 2}$ an, die

(a) den 1. und 3. Zeilenvektor vertauscht.

(b) das c-Vielfache des 3. Zeilenvektors auf den 2. Zeilenvektor addiert.