RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 3 / 30. Oktober 2012

AUFGABE 1:
Zeigen Sie, dass

Diffie-Hellman Problem $\Rightarrow$ *ElGamal Chiffretexte enschlüsseln* .

Hierbei bedeutet $A \Rightarrow B$, dass die Existenz eines effizienten Algorithmus für A die Existenz eines effizienten Algorithmus für B impliziert.

AUFGABE 2:
Wir betrachten das DL-Problem: Sei $\beta = \alpha^a \in \mathbb{Z}_p^*$, wobei $n = \text{ord}(\alpha)$ (von der Größenordnung von p) gegeben ist und a ermittelt werden soll. Konstruieren Sie einen Algorithmus, der bei Eingabe (p, α, β) die Ausgabe $a = \text{dlog}_\alpha(\beta)$ in $\mathbb{Z}_p^*$ in Zeit und Platz $\tilde{\mathcal{O}}(\sqrt{n})$ liefert. Nehmen Sie dazu an, dass n bekannt ist und beachten Sie, dass $a \bmod n$ definiert ist. Verwenden Sie die Meet-in-the-Middle-Technik.

AUFGABE 3:
Verwenden Sie Pollard's Rho-Methode, um den diskreten Logarithmus $\text{dlog}_2(6)$ in $\mathbb{Z}_{13}^*$ zu berechnen. Sei dafür $f : \mathbb{Z}_{13}^* \to \mathbb{Z}_{13}^*$ wie in der Vorlesung definiert und partionieren Sie $\mathbb{Z}_{13}^*$ in $S_1 = \{1, 2, 3, 4\}, S_2 = \{5, 6, 7, 8\}$ und $S_3 = \{9, 10, 11, 12\}$. Geben Sie für jeden Schleifendurchlauf i die Werte (s_i, x_i, y_i) und (s_{2i}, x_{2i}, y_{2i}) an.

AUFGABE 4:
Sei (p, α, β) wie zuvor. Betrachten Sie den Pollard Rho Algorithmus zur Berechnung von $\text{dlog}_\alpha(\beta)$ mit Startwert $s_0 = \alpha^0\beta^0$.

(a) Was passiert, wenn Sie die Menge S_3 ungeschickt wählen, so dass $1 \in S_3$ gilt?

(b) Um eine möglichst zufällige Abbildung f zu erhalten, könnte man auf die Idee kommen, die Mengen S_1, S_2, S_3 als eine echt zufällige Partition von $\mathbb{Z}_p^*$ zu definieren. Was ist an dieser Idee problematisch?