RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 2 / 26. Oktober 2011

AUFGABE 1:
Zeigen Sie, dass

$$\textit{Diffie-Hellman Problem} \Rightarrow \textit{ElGamal Chiffretexte enschlüsseln} \ .$$

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

AUFGABE 2:
Sei (p, α, β) ein öffentlicher Schlüssel des ElGamal Kryptosystems, d.h. $\beta = \alpha^a \bmod p$ für ein $0 \leq a \leq \text{ord}(\alpha) - 1$.

(a) Konstruieren Sie einen Algorithmus $\mathcal{A}$, der zur Eingabe (p, α, β) in Zeit und Platz $\tilde{\mathcal{O}}(\sqrt{\text{ord}(\alpha)})$ den diskreten Logarithmus $a = \text{dlog}_\alpha(\beta)$ in $\mathbb{Z}_p^*$ berechnet. Beachten Sie, dass a modulo $\text{ord}(\alpha)$ definiert ist. Sie dürfen bei der Konstruktion von $\mathcal{A}$ davon ausgehen, dass Sie die Ordnung $\text{ord}(\alpha)$ kennen.

b) Funktioniert der Angriff auch, wenn $\text{ord}(\alpha)$ unbekannt ist?

AUFGABE 3:
Wenden Sie Pollard's Rho-Methode zur Berechnung des diskreten Logarithmus manuell an. Berechnen Sie $\text{dlog}_\alpha \beta$ in $\mathbb{Z}_{31}^*$ für $\alpha = 7$ und $\beta = 28$. Es gilt $\text{ord}(\alpha) = 15$. Für die Berechnung der Abbildung $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ verwenden Sie folgende Mengen S_1, S_2, S_3:

$$S_1 := \{x \in \mathbb{Z}_p^* | x \equiv 0 \bmod 3\}$$
$$S_2 := \{x \in \mathbb{Z}_p^* | x \equiv 1 \bmod 3\}$$
$$S_3 := \{x \in \mathbb{Z}_p^* | x \equiv 2 \bmod 3\} \ .$$

Erstellen Sie eine Tabelle mit den Werten (s_i, x_i, y_i) sowie (s_{2i}, x_{2i}, y_{2i}) bis eine Kollision auftritt. Beginnen Sie bei $s_0 = \alpha^0 \beta^0$ mit $x_0 = y_0 = 0$.

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?