RUHR UNIVERSITÄT BOCHUM

RUB

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

Hausübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 3 / 30. Oktober 2012 / Abgabe bis spätestens 6. November 2012, 8:30 Uhr in dem Kasten auf NA 02

AUFGABE 1 (5 Punkte)**:**
Zeigen Sie, dass

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

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

AUFGABE 2 (5 Punkte)**:**
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

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

Hinweis: Es ist nützlich, die Identität $x \bmod y = x - y \cdot \lfloor \frac{x}{y} \rfloor$ zu benutzen.

AUFGABE 3 (5 Punkte)**:**
Schreiben Sie eine Funktion in sage, die den Pollard-Rho Algorithmus durchführt. Die Funktion soll als Eingabe ein Element α, die Ordnung von α, sowie ein Element β erhalten. Die Ausgabe der Funktion ist

$$x = \operatorname{dlog}_\alpha \beta \bmod \operatorname{ord}(\alpha).$$

(Wählen Sie die Partitionierung von $\mathbb{Z}_p^*$ als $S_1 = \{s \in \mathbb{Z}_p^* \mid s \equiv 0 \bmod 3\}, S_2 = \{s \in \mathbb{Z}_p^* \mid s \equiv 1 \bmod 3\}, S_3 = \{s \in \mathbb{Z}_p^* \mid s \equiv 2 \bmod 3\}$.)

Berechnen Sie mit Ihrem Algorithmus den diskreten Logarithmus von $\beta = 1580240$ zur Basis $\alpha = 897139$ in $\mathbb{Z}_p^*$ mit $p = 1827773$. Die Ordnung von α ist 456943. Wie viele Schritte sind nötig? Stimmt das mit der erwarteten Anzahl an Schritten überein?

AUFGABE 4 (5 Punkte)**:**
Sei $N = pq$ ein RSA-Modul mit $p < q$. Angenommen, wir haben eine zufällige Funktion $f : \mathbb{Z}_N \to \mathbb{Z}_N$. Zeigen Sie, dass die Faktorisierung von N in erwarteter Zeit $\tilde{\mathcal{O}}(N^{\frac{1}{4}})$ und Platz $\tilde{\mathcal{O}}(1)$ bestimmt werden kann.
Hinweis: Wenden Sie eine angepasste Pollard Rho-Methode an, d.h. finden Sie s_i, s_{2i}, $s_i \neq s_{2i}$ mit $s_i = s_{2i} \bmod p$.