

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 3 / 27. Oktober 2010

AUFGABE 1:

Zeigen Sie *ElGamal Chiffretexte entschlüsseln* \Leftrightarrow *Diffie-Hellman Problem*. Zeigen Sie dazu

1. Angenommen wir haben einen Algorithmus ELGAMAL, der bei Eingabe einer ElGamal verschlüsselten Nachrichten den Klartext ausgibt, d.h. $\text{ELGAMAL}(p, \alpha, \beta, \alpha^r, m\beta^r) = m$.

Zeigen Sie, dass man daraus einen Algorithmus DH konstruieren kann, der das Diffie-Hellman Problem löst, d.h. $\text{DH}(p, \alpha, \alpha^a, \alpha^b) = \alpha^{ab}$.

2. Angenommen, wir haben einen Algorithmus DH, der das Diffie-Hellman Problem löst, d.h. $\text{DH}(p, \alpha, \alpha^a, \alpha^b) = \alpha^{ab}$.

Zeigen Sie, dass man daraus einen Algorithmus ELGAMAL konstruieren kann, der bei Eingabe einer ElGamal verschlüsselten Nachrichten den zugrundeliegenden Klartext ausgibt, d.h. $\text{ELGAMAL}(p, \alpha, \beta, \alpha^r, m\beta^r) = m$.

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. Beschreiben Sie einen Meet-in-the-Middle Angriff auf a mit Zeit und Platz $\tilde{O}(\sqrt{n})$.

Verwenden Sie Ihren Algorithmus, um $\log_5(10)$ in \mathbb{Z}_{17}^* zu berechnen.

AUFGABE 3:

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

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