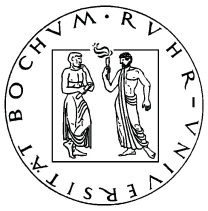
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann



Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2009

Blatt 1 / 22. April 2009

AUFGABE 1:
Beschreiben Sie einen aktiven Angriff (man-in-the-middle) auf das Diffie-Hellman Schlüsselaustauschprotokoll.
Können sich Alice und Bob vor einem MITM schützen, indem sie sich gegenseitig (verschlüsselte) Fragen zuschicken, die jeweils nur der andere beantworten kann ?

AUFGABE 2:
Zeigen Sie, dass die Schwierigkeit des DDH Problems relativ zu einer Gruppe $\mathcal{G}$ die Schwierigkeit des CDH Problems relativ zu $\mathcal{G}$ impliziert.

AUFGABE 3:
Betrachten Sie ein CPA-sicheres Public-Key Verfahren Π welches einzelne Bits verschlüsselt.

1. Zeigen Sie, dass ein unbeschränkter Angreifer mit Eingabe Public Key pk und Ciphertext $c \leftarrow Enc_{pk}(m)$ den Klartext m mit Wahrscheinlichkeit $1 - negl(n)$ bestimmen kann.

2. Zeigen Sie, dass der Chiffretext eines einzelnen Bits superlogarithmisch im Sicherheitsparameter ist. D.h. $|Enc_{pk}(b)| = \omega(\log n)$ für $b \in \{0, 1\}$.