6. Übungsblatt

SS 2015
Rechnersicherheit
Ausgegeben am 21.05.2015
Abgabe 28.05.2015

Marian Margraf
Inst. für Informatik
Freie Universität Berlin

Aufgabe 1. (Diffie-Hellman)

Geben Sie ein sicheres Schlüsselaustauschprotokoll unter Nutzung von Diffie-Hellman und Signaturverfahren an.

Aufgabe 2. (SPEKE)

Sei q eine Primzahl so, dass $p = 2q + 1$ ebenfalls eine Primzahl ist.
Zeigen Sie: Die Menge $\{x^2 \bmod p; x \in \mathbb{Z}_p^*\}$ bildet eine Untergruppe der Ordnung q.

Aufgabe 3. (Needham-Schroeder)

Beschreiben Sie die asymmetrische Version des Protokolls. Beschreiben Sie den von Lowe gefundenen Angriff auf diese Version. [1]

[1] Gavin Lowe, An Attack on the Needham-Schroeder Public-Key Authentication Protocol (1995) (`http://web.cs.wpi.edu/~cs564/f12/papers/lowe95.pdf`)