Technische Universität München
Fakultät für Informatik
Prof. Dr. H. Seidl

Dr. K. N. Verma
verma@in.tum.de
Room: MI 02.07.041

Cryptographic Protocols

Winter Semester 2005

2. Homework *8 November 2005*

Exercise 1:

The *client certificate* and *certificate verify* messages are optional in the TLS handshake protocol. Show how this leads to an attack where the attacker pretends to be another client.

Exercise 2:

Consider the following Ping-Pong protocol. Apply the analysis developed in the lecture on this protocol.

$$\begin{array}{ll} X \to Y\colon & \{\{M\}_{K_Y}, X\}_{K_Y} \\ Y \to X\colon & \{M\}_{K_X} \end{array}$$