Technische Universität München
Fakultät für Informatik

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

Language Based Security

Summer Semester 2006

9. Homework *12 July 2006*

Exercise 1:

Find an attack against the following protocol. N_a is a fresh nonce chosen by A in each session and sent to B who then acknowledges it. The goal is for A and B to agree on N_a as a common secret between them. K_a and K_b are public keys of A and B respectively.

$$\begin{array}{l} A \longrightarrow B : \{N_a\}_{K_b}, A \\ B \longrightarrow A : \{N_a\}_{K_a} \end{array}$$