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

6. Homework — *22 December 2005*

Exercise 1:

Consider the following variant of Lowe's fix to the Needham Schroeder Public key protocol.

$$\begin{array}{ll} A \to B: & \{A, N_a\}_{K_b} \\ B \to A: & \{B \oplus Na, N_b\}_{K_a} \\ A \to B: & \{N_b\}_{K_b} \end{array}$$

where $\oplus$ is the exclusive-or operation. As before we consider the Dolev-Yao model extended with rules for exclusive-or.

a) Find an attack against this protocol.
b) Consider the approximation of finitely many nonces and describe the intruder's knowledge using push and pop rules, in presence of the $\oplus$ operation.

Exercise 2:

Let Σ be a set of constants and let S be a set of terms of the form $a_1 \oplus \ldots \oplus a_n$ where each a_i is from S. Let m be a term of the same form. Show how to decide whether the intruder can obtain m by applying exclusive-or operations repeatedly, starting with the terms in S.