Technische Universität München *Dr. K. N. Verma*
Fakultät für Informatik *verma@in.tum.de*
Prof. Dr. H. Seidl *Room: MI 02.07.041*

Cryptographic Protocols

Winter Semester 2005

5. Homework *15 December 2005*

Exercise 1:

Show that the result on the reduction of number of agents allows us to decide secrecy in the presence of a passive attacker (for unbounded number of sessions and nonces).

Exercise 2:

Consider the following protocol where $\oplus$ is the xor operation, and S_{ab} is a long term secret between A and B.

$$\begin{aligned} A &\longrightarrow B : N_a \oplus K_{ab} \\ B &\longrightarrow A : N_b \oplus N_a \\ A &\longrightarrow B : S_{ab} \oplus N_b \end{aligned}$$

The properties of xor operation are as follows:

$$\begin{aligned} x \oplus (y \oplus z) &=_{xor} (x \oplus y) \oplus z \\ x \oplus y &=_{xor} y \oplus x \\ x \oplus 0 &=_{xor} x \\ x \oplus x &=_{xor} 0 \end{aligned}$$

To take into account the xor operation in the intruder deduction problem, we add the following inference rules to the existing rules:

$$\frac{E \vdash m \quad m =_{xor} m'}{E \vdash m'} \qquad\qquad \frac{E \vdash m_1 \quad E \vdash m_2}{E \vdash m_1 \oplus m_2}$$

Does the protocol preserve the secrecy of the message S_{ab}?