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

4. Homework — *22 November 2005*

Exercise 1:

Consider the following ping-pong protocol

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

a) Describe the protocol using multiset rewriting rules as discussed in the lecture, using predicates $A_0(\_,\_), B_0(\_,\_), A_1(\_,\_,\_), \ldots$.

b) Consider the security property

$$Ha(x), Ha(y), A_2(x, y, z), I(z)$$

Suppose agents cannot speak to themselves. Write down an attack against this security property.

c) Now we allow agents to speak to themselves. Project the above attack as discussed in the lecture to obtain an attack involving two agents.

Exercise 2:

Consider arbitrary ping-pong protocols modeled as usual, with agents disallowed to speak to themselves.

a) For the security property

$$Ha(x), A_2(x, y, z), I(z)$$

what is the minimum number of agents required to find an attack ?

b) For the security property

$$A_2(x, y, z), I(z)$$

what is the minimum number of agents required to find an attack ?