Technische Universität München
Fakultät für Informatik

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

Language Based Security

Winter Semester 2008

Exercise sheet 5. *26 Nov 2008*

Exercise 1:

Consider the following protocol, where K_A and K_B are the public keys of A and B respectively, and M is a secret that A wants to communicate to B.

$$A \longrightarrow B : \{M\}_{K_B}, A$$
$$B \longrightarrow A : \{M\}_{K_A}$$

a) Show that secrecy of M is not ensured by the protocol.

b) Model the protocol as a Spi-calculus process $P(x)$, where x is a variable (representing M in the above description) whose secrecy we are interested in. For this model the two participants as two processes running in parallel. Use the `repeat` construct of the Spi calculus to model the fact that there can be arbitrarily many sessions.

c) Show that secrecy of x is not ensured, by finding some M_1 and M_2 such that $P(M_1/x) \simeq P(M_2/x)$ does not hold.