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

3. Homework *15 November 2005*

Exercise 1:

Consider the following set of messages known to the intruder:
$\{\{m_1\}_{m_5}\}_{\langle m_2,m_3\rangle} \quad \{m_5\}_{m_6} \quad \{m_2\}_{m_4} \quad \{m_3\}_{m_4} \quad m_4$

a) Write the set of push and pop rules to describe the set of messages the intruder can deduce.
b) Apply the operations discussed in the lecture to add more rules.
c) Finally use the push rules to check whether the messages $\{m_1\}_{m_5}$ and m_1 can be computed by the intruder.

Exercise 2:

Given a set of push rules, show that the nonemptiness of a state can be checked in linear time.