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 4. *19 Nov 2008*

Exercise 1:

If an attacker knows a certain set of messages then he can compute other messages from them by performing encryptions, decryptions, pairings, decompositions, etc. For example if the attacker knows the messages a, b and $\{c\}_{\langle a,b\rangle}$ then he can compute c (assuming symmetric encryption). Formally we consider the following syntax of messages, where c denotes some constant from a set $\mathcal{C}$.

$$m ::= c \mid \langle m_1, m_2 \rangle \mid \{m_1\}_{m_2}$$

For simplicity we consider only symmetric encryption. We write $T \vdash m$ to say that the message m can be computed from the set T of messages. This is defined as follows.

- If $m \in T$ then $T \vdash m$.
- If $T \vdash m_1$ and if $T \vdash m_2$ then $T \vdash \langle m_1, m_2 \rangle$.
- If $T \vdash m_1$ and if $T \vdash m_2$ then $T \vdash \{m_1\}_{m_2}$.
- If $T \vdash \langle m_1, m_2 \rangle$ then $T \vdash m_1$.
- If $T \vdash \langle m_1, m_2 \rangle$ then $T \vdash m_2$.
- If $T \vdash \{m_1\}_{m_2}$ and $T \vdash m_2$ then $T \vdash m_1$.

Give an algorithm which decides whether $T \vdash m$ for a given finite set T of messages and a message m. What is the time complexity of the algorithm?