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

1. Homework — *25 November 2005*

Exercise 1:

Consider the following modified version of the Needham-Schroeder public key protocol where both nonces N_a and N_b are sent in the third message.

1. $A \longrightarrow B : \{A, N_a\}_{K_b}$
2. $B \longrightarrow A : \{N_a, N_b\}_{K_a}$
3. $A \longrightarrow B : \{Na, N_b\}_{K_b}$

What are the security properties of this protocol ?

Exercise 2:

Given positive integers a, x and n, show that the value $a^x \bmod n$ can be computed in time polynomial in the total number of bits in the binary representation of the integers.

Exercise 3:

Define *generalized graphs* to be of the form $G = (V, E)$ where V is a set of *vertices* and E is a set of *edges* of the form $v_1, \ldots, v_n \Rightarrow v_0$ where $n \geq 0$ and v_i are vertices. The set of *reachable* vertices in G is defined inductively by the following rule: if $v_1, \ldots, v_n \Rightarrow v_0$ is an edge in E and v_i is reachable for $1 \leq i \leq n$ then v_0 is reachable. It can be decided in linear time whether a vertex is reachable in such a graph.

Use this to show that the intruder deduction problem can be solved in linear time.