Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

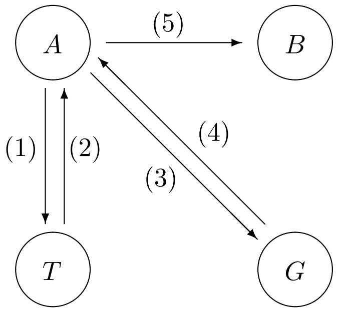
Tutorial 10

Friday, January 22, 2016

Problem 1. *(Kerberos with ticket granting server)* We introduce a ticket granting server for the simplified Kerberos protocol.
To establish secure *unilateral* authentication from A (Alice) to B (Bob) with a trusted authority server T (Trent) and a ticket granting server G (Grant), we use the following parameters:

- k_{AT} is a shared key between A and T
- k_{AG} is a session key for secure communication between A and G
- TGT is a ticket granting ticket to authenticate A to G
- k_{TG} is a shared key between T and G
- a_{AG} is an authenticator between A and G
- k_{AB} is a session key for secure communication between A and B
- k_{BG} is a shared key between G and B
- ST is a service ticket to authenticate A to B
- a_{AB} is an authenticator between A and B
- Time stamps t_i and validity periods l_i, for $i = 1, 2, \ldots$

The sequence of messages to be exchanged by the protocol is provided in the figure below.



Formulate[1] the corresponding protocol and describe it with the parameters as given above.

[1] Feel free to use textbooks, www, etc.

Problem 2. *(Feige-Fiat-Shamir-signature)* Zero-knowledge-protocols can also be used to construct signature schemes. Construct a signature scheme from the Feige-Fiat-Shamir identification protocol by replacing the challenge $(b_1, ..., b_k)$ with a hash value $h(m, x)$. Specify the signing and the verification algorithm.

Problem 3. *(zero-knowledge factorization)* James Bond (JB) wants to prove to the British secret service (MI5) that he knows the factorization of a composite number n without revealing the factors. These factors are two distinct primes p and q fulfilling the congruences $p, q \equiv 3 \pmod 4$. JB suggests the following protocol:

(i) The MI5 chooses an arbitrary quadratic residue y modulo n, and sends y to JB.

(ii) JB computes the square root x of y, and sends x to the MI5.

(iii) The MI5 checks whether $x^2 \equiv y \pmod n$.

These steps are repeated 20 times. If JB can compute the square roots modulo n in all 20 attempts, the MI5 believes him.

a) Show that the MI5 can factor n with very high probability.

b) Does this protocol satisfy the requirements of a zero-knowledge protocol?

c) Is a third party able to derive useful information about the factorization of n by intercepting the communication between JB and the MI5?