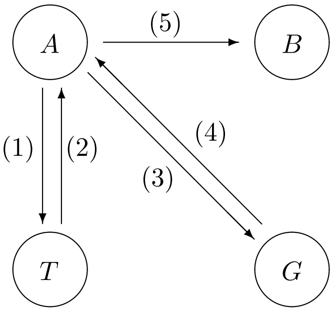
RWTH AACHEN UNIVERSITY Lehrstuhl für Theoretische Informationstechnik

Homework 12 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Georg Böcherer, Henning Maier

18.01.2011

Exercise 37. We introduce a ticket granting server for the simplified Kerberos protocol. Devise a protocol to establish secure *unilateral* authentication from A to B with a trusted authority server T and a ticket granting server G by using the following parameters:
A, B, T and G are identifiers, k_A 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_G 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_B is a shared key between G and B, ST is a service ticket to authenticate A to B and a_{AB} is an authenticator between A and B. Use timestamps t_i and validity periods l_i, $i = 1, 2, ...$, if necessary. Specifiy tickets and authenticators. The sequence of messages is provided in the figure below.



Exercise 38. James Bond wants to prove to the British secret service (MI5) that he knows the factorisation of a composite number n without revealing the factors. These factors are two distinct primes p and q fulfilling $p, q \equiv 3 \pmod 4$. He suggests the following protocol:

(i) The secret service chooses an arbitraty quadratic residue y modulo n, sends y to James.

(ii) James computes the square root x of y, sends x to the secret service.

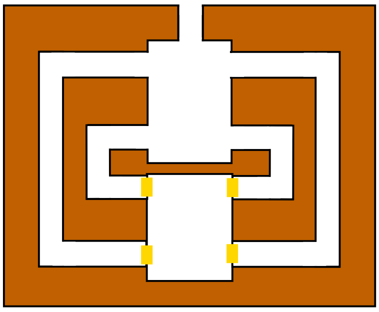
(iii) The secret service checks, whether $x^2 \equiv y \pmod n$.

These steps are repeated 20 times, if James can compute the square roots modulo n in all 20 attempts, the secret service believes him. Show that the secret service can factor n with very high probability. Is this protocol a zero-knowledge protocol? Is a third party able to derive useful information about the factorisation of n by intercepting the communication between James and the secret service?

Exercise 39. Zero-knowledge-procols can also be used to construct signature schemes. Construct a signature scheme from the Feige-Fiat-Shamir identification protocol by replacing the challenge $(b_1, \ldots, b_k)$ with a hash value $h(m, x)$.

Specify the signing and the verification algorithm.

Exercise 40. [1] Consider the diagram of tunnels in the figure below.



Suppose each of the four yellow doors to the central chamber is locked so that a key is needed to enter, but no key is needed to exit. Peggy claims she has the key to one of the doors. Devise a zero-knowledge protocol in which Peggy proves to Vince that she can enter the central chamber. Vince should obtain no knowledge of which door Peggy can unlock.

[1] This exercise is optional and will not be presented in the tutorial.