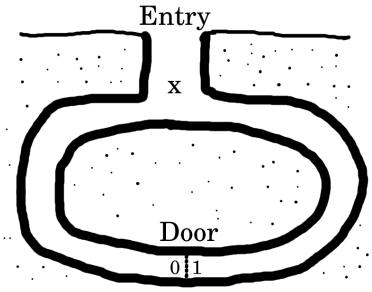
T-79.159 Cryptography and Data Security **Spring 2004**
Tutorial 8
Thursday 25.3.2004 14.15, room T3.
Markku-Juhani O. Saarinen <mjos@tcs.hut.fi>

1. We start with a classic example of a zero-knowledge proof by Quisquater and Guillou, called "The Ali Baba's Cave".

   Consider a cave of the following shape:

   Two persons, Alice and Bob, are standing at point x. Alice claims that she knows the magic words to open the door ("Open Sesame"), but doesn't want to reveal them to Bob. The door is far away and no sound from there can be heard at x. The door opens both ways. Design an interactive, randomized zero-knowledge proof that Alice can use to convince Bob that she knows the magic words (with high probability) without actually revealing them to Bob.

2. Design a joint 2-party method for generating a n-bit (probable) prime number, using the joint coin tossing method (slide 33 of Lecture 8) as a primitive. Here we assume that neither party can stop the protocol at any point and that the communication is secure and reliable.

3. It is generally assumed that distinguishing quadratic residues form quadratic nonresidues (mod n) is a hard problem when n is a product of large primes. The problem becomes easy if the factorization of n is known.

   Let n be a product of large primes and x be a known quadratic nonresidue (mod n). Consider and prove the following scheme for a zero-knowledge proof of Q.R. (mod n):

   - Victor the Verifier generates random numbers z_i, $0 < z_i < n$ and random bits b_i. Victor sends Peggy the Prover the tuple $(w_1, w_2, \cdots, w_k)$, where $w_i = x^{b_i} z_i^2 \mod n$.
   - Peggy replies with the tuple $(c_1, c_2, \cdots, c_k)$, where

     $$c_i = \begin{cases} 0 & \text{when } w_i \text{ is a q.r.} \\ 1 & \text{when } w_i \text{ is a q.n.r.} \end{cases}$$

   - Victor accepts the proof if $b_i = c_i$, $1 \leq i \leq k$.

   What is the probability of Peggy being able to "fake it" ? Is it possible to design a protocol if a quadratic nonresidue x is not known ?