T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 7
Tue 25.3.2003 12–14 T3 and Wed 26.3.2003 18–20 T1

1. **Suppose that you have shamanistic powers and you can control the local weather to the extent that you can make it a) rain or b) not rain on the following day. How could you interactively prove this to a understandably suspicious scientist (without revealing your secret magical methods) so that he can be 99.9% sure about this – and how long would it take ?**

   In the interactive proof system Peggy the Shaman asks for one bit of information from Victor the Scientist on each day; whether he wants it to rain on the following day or not. Victor can make the choice any way he wants.

   Clearly, if Victor chooses the bit appropriately, the probability Peggy "successfully faking it" falls by 50% on each day. So after 10 days, the probability is 0.098%, and Victor is more than 99.9% convinced. The problem for Peggy is that *only Victor is convinced.*

2. **Discuss a *bit commitment scheme* using a collision-resistant function – say SHA-1.**

   Let $H()$ be the hash function and m is the message.

   Many erroneous techniques are sometimes this problem. One of the most obvious ones is that the sender commits $H(m)$ first and then reveals the commitment m. Clearly, if m is very short, information regarding it is leaked to the recipient.

   Rather, it makes sense for the sender to pick a random string r, and commit $H(r \mid m)$. Commitment can be revealed by $r \mid m$.

   This works for Davies-Meyer hashing modes, but more advanced techniques are recommended, see Shai Halevi, Silvio Micali: *Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing.* Proc. CRYPTO 1996: 201 – 215.

3. **Design a practical protocol for flipping an k-sided dice fairly, where k is a small integer. You may use the commitment scheme from previous problem.**

   We implement the protocol from the previous problem.

   1. Alice picks a random number $0 \leq a < k$ and commits it to Bob.
   2. Bob picks a random number $0 \leq b < k$ and commits it to Alice.
   3. Both reveal their commitments. The dice value is computed as $(a + b) \mod k$.

   Of course in this example it might make sense to commit bigger random strings and compute the value from an output of a one-way function of the concatenation of these strings, but such a scheme would be information-theoretically as secure as the one given above.

4. **Design a protocol for a zero-knowledge proof of factorization (which we assume to be equivalent to QR problem) of $n = pq$, where the verifier only knows one quadratic non-residue modulo n (but not the factorization).**

   We note that the QR - based interactive proof from the slides can be adopted for this purpose.

   Here Victor the Verifier has one quadratic non-residue x modulo n, and Peggy the Prover tries to convince him that she knows the secret factorization $n = pq$.

   1. Victor generates k random numbers $z_i \in \mathbb{Z}_n^*$ and k random bits b_i, and sends $(w_1, w_2, \cdots, w_k)$ to Peggy, where

   $$w_i = x^{b_i} z_i^2 \mod n$$

   2. Peggy responds with a bit string $(c_1, c_2, \cdots, c_k)$ indicating which w_i were quadratic residues (0) or non-residues (1).
   3. Victor accepts if $b_i = c_i$.

   We first note that with the factorization of n, it is easy to determine whether a number w_i is a quadratic residue or not. One simply computes the Legendre / Jacobi / Kronecker (which ever name you like) symbols $(\frac{w_i}{p})$ and $(\frac{w_i}{q})$ – if either is -1, then w_i is a quadratic non-residue modulo n. Fast algorithms exist for computing this, even faster than those given by the equation $(\frac{x}{p}) = x^{(p-1)/2} \mod p$. It is indeed believed that this problem (quadratic residuosity) is equivalent to factorization, although this hasn't been proved.

   In step 1., by multiplicativity of Legendre symbol, the values w_i are non-residues only when $b_i = 1$. Victor therefore only needs x to generate the challenge, not the factorization.