Introduction to Cryptography – Exercise no. 5

Submit in Pairs/Single to **mailbox** 19 by 27/1/13, 1:00 p.m.

1. This question deals with weaknesses of the ElGamal signature scheme.

   (a) Show that given a legal signature (R, S) on a message m, an adversary can compute signatures for messages of the form $m' = (m + bS)a \bmod p - 1$, for an arbitrarily chosen $b \in Z_p^*$ and $a = g^b \bmod p$.

   (b) Show that the ElGamal scheme is vulnerable to existential forgery attack. Show that an adversary can produce a combination of a message m and a legal signature on it (R, S), but he cannot necessarily choose the value of m.
   Hint: Choose R to be of the form $R = g^{\alpha+\beta x} \bmod p - 1$ for some $\alpha, \beta \in Z_p^*$, such that $gcd(\beta, p-1) = 1$ (in practice, α and β are chosen randomly).

   (c) Show that if the same value r is used with two ElGamal signatures on two different messages m_1 and m_2, then the private key X_U can be computed. In other words, given (m_1, R, S_1) and (m_2, R, S_2), where $m_1 \neq m_2$, X_U can be found.

   (d) Show that if the signer chooses r of a signature randomly, and then increments it by one to sign an additional message, then given these two ElGamal signatures (on two different messages m_1 and m_2), the private key X_U can be computed.

2. In this question we discuss variants of the Rabin method for signing. Let p, q be large prime numbers and let the public key be $n = pq$. Given a message $m \in Z_n$ to sign, we find a square root b of m, i.e., b such that $b^2 \equiv m \bmod n$. In case such a square root does not exist, we concatenate a random string r to m and find the square root of $m||r$.

   Assume that the owner chooses 2 prime numbers $p \equiv 3 \bmod 8$ and $q \equiv 7 \bmod 8$, calculates $n = pq$, and publishes n as his public key for signing.

   (a) Show that for all $m \in Z_n$ exactly one of $m, -m, 2m, -2m$ is a QR modulo n.
   Hint: Show that -1 and 2 are QNRs modulo p, that -1 is a QNR modulo q and that 2 is a QR modulo q.

   In Rabins method for signing we calculate the square root of the message m. A problem arises when $m \in QNR_n$. The following solution is suggested: the signer identifies which of the 4 values $m, -m, 2m, -2m$ is a QR modulo n.

   (b) Explain how.

   Denote this QR by ℓ. The signer calculates the square root of ℓ modulo n.

   (c) Explain how.

   And sends one of the roots as a signature.

(d) How does the signature verification is performed?

(e) Explain why such a root is, in fact, a signature on 4 different messages. Which messages?

In order to ensure that signatures do not leak additional signatures on 3 different messages, it was suggested to choose the message m from the interval $(\frac{n}{8}, \frac{n}{4})$.

(f) Show that if one chooses m from the above interval, then the message cannot be considered, mistakenly, as a signature on another message.

3. When Peggy wants to prove her identity to Vic, the following steps are repeated t times:

   - Peggy chooses two large prime numbers p and q, and publishes $n = pq$ and some $x \in QNR(n)$. Peggy is going to prove that she knows the factorization of n by being able to find efficiently whether some given z is in $QR(n)$ or $QNR(n)$.
     (a) Vic chooses $v \in Z_n$ randomly and computes $y \equiv v^2 \bmod n$, chooses a bit $i \in \{0, 1\}$, randomly, and sends $z \equiv x^i y \bmod n$ to Peggy.
     (b) If $z \in QR(n)$ then Peggy defines $j = 0$, otherwise, $j = 1$, and sends j back to Vic.
     (c) Vic checks whether $i = j$.
   - Vic accepts the proof if the check succeeded in all t times.

   (a) Show how Oscar (a cheater) can use the protocol to receive information he can not compute by himself.

   (b) Here is a simulator to this protocol:
      i. T is the transcript of the conversation, and in the beginning we initialize $T = (x, n)$.
      ii. Repeat t times:
         A. Choose i, y, v and z like Vic.
         B. Concatenate (z, i) to T.

      Show that the output distribution of the simulator is <u>equal</u> to the distribution of a real communication with Peggy.

   (c) Is this a Zero-Knowledge Protocol?
   If you answer yes, explain how is it that Oscar can use this protocol to gain information that he cannot compute by himself. If you answer no, explain what is wrong with the simulator, as it has the same distribution of outputs as in the protocol.