Cryptography

Problem set 9 - 21-22 V 2015

1. Show how to transform RSA blind signature scheme into a 1-out-of-2 oblivious transfer protocol.
2. (a) For the Chaum-Pedersen commitment scheme with $p = 37, g = 13, h = 35$, a commitment $c(x, r) = g^x h^r \bmod p = 29$ was published. Find value x to which $c(x, r)$ commits to.

   (b) For the commitment scheme based on DL in Z_p, with parameters $p = 37, g = 13$ a commitment $c(x) = g^x \bmod p = 29$ was published. Find x.
3. Prove security of Feige-Fiat-Shamir idenfitiaction scheme. Why it is better than Fiat-Shamir identification scheme?
4. A participant of a protocol ($\mathbf{P_i}$) has a secret s_i. To share a secret, a participant chooses at random a prime p, and then picks uniformly at random $r_{i,1}, r_{i,2} \in Z_p$, and computes

   $$r_{i,3} = s_i - r_{i,1} - r_{i,2} \bmod p.$$

   Then $\mathbf{P_i}$ sends $r_{i,a}, r_{i,b}$ (for $a, b \neq j$) to a participant $\mathbf{P_j}$ (*i.e.,* $\mathbf{P_1}$ sends $r_{1,1}, r_{1,3}$ to $\mathbf{P_2}$).

   Show that neither $\mathbf{P_2}$ nor $\mathbf{P_3}$ learn s_1. How any two participants are able to compute s_i?

   Assuming that s is an ElGamal's private signature key (and $g, h = g^s \bmod p, p$ is a corresponding public key) show how $\mathbf{P_i}$ i $\mathbf{P_j}$ can cooperate to sign a message m.
5. Present problem statement, solution and security analysis of Yao's Millionaire problem.
6. Present problem statement, solution and security analysis of Socialist Millionaire problem.
7. Present problem statement, solution and security analysis of Chaum's Dining Cryptographers.