Cryptography cs 4995
Instructor: Prof. Michael Rabin

Problem Set 5

Due: Tuesday, Apr. 24 2007

1. **(Paillier Encryptions)** Suppose a prover presents cyphertexts $C = E_n(x, r), C_1 = E_n(x_1, r_1)$ and $C_2 = E_n(x_1, r_2)$ which are Paillier encryptions for x, x_1 and x_2. The prover wants to prove to a verifier that $x \in \{x_1, x_2\}$ (i.e. that C is an encryption of the same message as either C_1 or C_2 without revealing the values x_1 and x_2. Give a protocol that achieves this. Hint: We may use test sets. The prover prepares a test set by choosing s_1, s_2 randomly from $\mathbb{Z}_n^*$ and creating $TS = \{\overline{C_1}, \overline{C_2}\}$ where $\overline{C_1} = C_1 \cdot s_1^n \pmod{n^2}$ and $\overline{C_2} = C_2 \cdot s_2^n \pmod{n^2}$. The prover permutes the pair for sending the test set to the verifier.

   (a) Prove that $\overline{C}_1$ and $\overline{C}_2$ encrypt x_1 and x_2.

   (b) Show that if the verifier knows the test set is valid, the prover can give a zero knowledge proof that $x \in \{x_1, x_2\}$.

   (c) But the verifier does not know the test set is a proper oen. Show and explain how the method given in class overcomes this problem.

2. **(Discrete Logarithm)** Let G be a multiplicative cyclic group of order q, where q is a large prime. Show that if there exists a randomized algorithm that given three random elements $g_1, g_2, g_3 \in G$, produces with probability $1/2$ a triple a_1, a_2, a_3, not all 0, such that $g_1^{a_1} g_2^{a_2} g_3^{a_3} = 1$, then the discrete logarithm problem is efficiently solvable in G.

3. **(Mental poker)** For questions 2–4, consider the following protocol for playing poker:

   5 people are going to play poker over the Internet as follows: fix $p = 2q + 1$ with p, q prime. Let $g \in \mathbb{Z}_p^*$ be a generator of $\mathbb{Z}_p^*$. The cards will be represented by $g_1, \ldots, g_{52} \in \mathbb{Z}_p^*$ where $g_i = g^{b_i}$ and the $\{b_i\}$ are all distinct. (All players know which elements represent which cards.)

   To begin, player 1 takes the list of cards $g_1, \ldots, g_{52}$, chooses a random exponent a_1 relatively prime to $p - 1$, computes $g_{i,1} = g_i^{a_1}$ for $1 \le i \le 52$, and randomly permutes the result. This gives a new list of cards $g_{1,1}, \ldots, g_{52,1}$ which is then sent to player 2.

   Player 2 takes the list $g_{1,1}, \ldots, g_{52,1}$, chooses a random exponent a_2 relatively prime to $p - 1$, computes $g_{i,2} = g_{i,1}^{a_2}$ for $1 \le i \le 52$, and randomly permutes the result. This gives a new list of cards $g_{1,2}, \ldots, g_{52,2}$ which is then sent to player 3. Players 3, 4, and 5 do the same until the cards are passed back to player 1.

   Player 1 now chooses five of the elements from the list $g_{1,5}, \ldots, g_{52,5}$ that he is given. Say he picks "cards" $h_1, \ldots, h_5$. He passes the remaining elements on the list to player 2 who chooses five cards and so on. All players can view all communication between any of the other parties.

To play, the players have to learn what cards they hold. This can be done as follows: player 1, for example, sends his cards $h_1, \ldots, h_5$ to player 2 who computes $h_{i,2} = h_i^{a_2^{-1}}$ for $1 \leq i \leq 5$. The results are passed to player 3 who computes $h_{i,3} = h_{i,2}^{a_3^{-1}}$ for $1 \leq i \leq 5$. It continues in this way until player 5 hands back "cards" $h_{1,5}, \ldots, h_{5,5}$ to player 1. Now, player 1 computes $h_i^* = h_{i,5}^{a_1^{-1}}$ for $1 \leq i \leq 5$. Player 1 has now learned the values $h_1^*, \ldots, h_5^*$ of his cards. (Verify for yourself that this works.)

(a) Show that this protocol is flawed if the original representation $g_1, \ldots, g_{52}$ of the cards is not chosen carefully. (Hint: Consider how certain cards might be "marked". More specifically, consider what property of a card remains unchanged after raising a card to a random, odd exponent.)

(b) After the game is played, how can it be verified that no one cheated? (Recall that *all* communication is public and assume it is remembered by all parties.)

(c) If there is (are) cheater(s), how can they be identified after the game is played?