Advanced Topics in Cryptography

Final Homework
Due by July 4, 2006

1. In the lecture we showed a 4-server PIR protocol with $O(n^{1/3})$ communication. Design a similar protocol for 8-server PIR and try to minimize its communication overhead.

2. This question investigates the Cramer-Shoup cryptosystem. Consider a variant of this system in which the decryption process does not include the consistency check. Namely, where given a ciphertext $\langle u, v, e, w \rangle$ the decryption process simply outputs $e/(u^x v^y)$. Show exactly where the proof of security fails.

3. Consider a protocol for bidding in an auction where the seller publishes a public key PK and each player sends an encryption $E_{PK}(x)$ of its bid x.

   Show a chosen-plaintext secure encryption system E, such that there is an algorithm which given PK and a ciphertext $y = E_{PK}(x)$ can generate a ciphertext y' of the plaintext $x + 1$. You cannot assume that the algorithm knows x. Explain how a bidder might try to cheat in the protocol using this algorithm.

   Show that this problem does not exist with encryption systems which provide chosen-ciphertext security. Namely, show that if $E()$ provides chosen-ciphertext security it is impossible to change $E(x)$ to $E(x+1)$ with more than negligible success. Try to formulate this statement as accurately as possible, and prove it. (Hint: show that if it is possible to change $E(x)$ to $E(x+1)$ then it is possible to attack the chosen-ciphertext security of E.)

4. This question investigates the Decisional Linear Diffie-Hellman assumption:

   Decisional Linear Diffie-Hellman assumption: Let G be a group of order p. Let u, v, h, s be randomly chosen generators of G, and let a, b be random elements in $[1, p]$. Then it is hard for any polynomial time algorithm to distinguish between the tuples $\langle u, v, h, u^a, v^b, h^{a+b} \rangle$ and $\langle u, v, h, u^a, v^b, s \rangle$. (In other words, given $\langle u, v, h, u^a, v^b, h^c \rangle$ it is hard to decide whether $c = a + b \bmod p$.)

   Question 4.a: Show that an algorithm for solving the Decisional Linear Diffie-Hellman problem in G gives an algorithm for solving the Decisional Diffie-Hellman problem in G.

   It is believed that the converse in not true. Namely, that the Decisional Linear Diffie-Hellman problem is hard even in groups in which the DDH problem is easy. This motivates the construction of an encryption scheme based on the Decisional Linear Diffie-Hellman assumption. This encryption scheme works as follows:

   Public key generators u, v, h of G.
   Private key exponents $x, y \in [1, p]$ such that $u^x = v^y = h$.
   Encryption To encrypt a message $m \in g$ choose random $a, b \in [1, p]$ and output triple $\langle u^a, v^b, m \cdot h^{a+b} \rangle$.
   Decryption To decrypt $\langle T_1, T_2, T_3 \rangle$ compute $T_3/(T_1^x \cdot t_2^y)$.

   Question 4.b: Show how the user can generate the private and public keys.

   Question 4.c: Show that decryption is always correct.

   Question 4.d: Show that this encryption system is semantically secure against a chosen-plaintext attack, assuming that the Decisional Linear Diffie-Hellman assumption holds.