CSE 590 YA: Practical Aspects of Modern Cryptography
Winter 2002

Assignment #7

Due in class: Tuesday, February 26

1. Suppose that a secret in the range $Z_{11} = \{0, 1, \ldots, 10\}$ has been shared using Shamir's threshold scheme among five individuals so that any three of the five can reconstruct the secret. Shareholder 2 reveals the share value 1, shareholder 4 reveals the share value 6, and shareholder 5 reveals the share value 1 (same as shareholder 2). Compute the value of the secret. Show your work.

2. We showed in class that for any of the secret sharing methods we discussed, an additive homomorphism exists (that sums of shares of secrets constitute shares of the sum of the secrets). For which of the three methods we discussed (AND, OR, and THRESHOLD) does a multiplicative homomorphism exist? Describe why this is or is not the case.

3. Suppose that Alice wants to convince Bob that a value Z that she will give him is either an encryption of X or an encryption of Y (where Alice holds the encryption key). Describe how she can do this *without* revealing to Bob which of X or Y the value she gives him is an encryption of.

4. Suppose again that Alice wants to give Bob a value Z that is an encryption of either X or Y without revealing which is the case. Suppose further that there is a method by which Alice can demonstrate to Bob that two different values are encryptions of the same value — without revealing this decrypted value. Describe how Alice can convince Bob that, with error probability at most 2^{-100}, the value she gives Bob is an encryption of either X or Y.

5. Suppose now that Alice wants to broadcast a value Z that is an encryption of either X or Y without revealing which is the case. Again assume that Alice has a method for proving that two encryptions are actually distinct encryptions of the same value. Describe how Alice can broadcast, for any passive observer to see, a value Z along with a convincing "proof" that Z is indeed an encryption of either X or Y.