ECS 227: Modern Cryptography
Homework 1

Phillip Rogaway

Out: 11 January 1996. Due: 23 January 1996

1. Suppose parties A, B and C can each toss up to one million fair coins (a fair coin lands heads or tails equiprobably). They have no other source of randomization. Show that the there is no protocol for A, B and C to run which will elect one of them as a leader, with all three players being elected equiprobably. Exhibit a protocol which *almost* achieves this, assuming A, B, and C are honest. What is the probablity that your protocol *fails*?

2. Party D (the dealer) shuffles a deck of 52 cards, then deals out the deck to players N, S, E, and W. Find a method by which, with constant probablity, N can communicate a bit b to S. Neither E nor W should have any idea of what is the bit b (beyond its *a priori* probablity). All communication must be in the open, according to a specified protocol.

3. In class we described the *dating problem.* **Part A.** Find a simple solution in the physical world. Assume both Alice and Bob are honest. You can instruct a player to shuffle cards, flip coins, say what s/he wishes to the other player, etc.. You may not use any "trusted intermediary," nor can you instruct a player to "forget" something which s/he has seen or heard, nor can you instruct a player to "not listen," etc.. **Part B.** Carefully define what it would mean to have a *communications protocol* which solves the dating problem. Again, assume that both Alice and Bob are honest. Assume they communicate over a clear channel. **Part C.** Can you find a communications protocol to solve the dating problem?