ECS 227 — Modern Cryptography — Winter 2000
Problems 1–2

Phillip Rogaway
Out: 6 January 2000. Due: 13 January 2000.

1. **A limitation on fixed-time fair-coin-flipping TMs.** Cosider the model of computaion in which we agument a Turing machine so that it can obtain the output of a random coin flip: by going into a distinguished state $Q_{\$}$, the next state will be Q_{H} with probability $1/2$, and the next state will be Q_{T} with probablity $1/2$. Show that, in this model of computation, there is no constant-time algorithm to perfectly deal out five cards to each of two players.

   (A deck of cards consists of 52 cards, and a fair deal means that all hands should be equally likely. Saying that the algorithm is constant-time means that there is some number T such that the algorithm is guaranteed to stop within T steps.)

2. **Encryption with a deck of cards.** Alice shuffles a deck of cards and deals it all out to herself and Bob (each of them gets half of the 52 cards). Alice now wishes to send a secret message M to Bob by saying something aloud. Eavesdropper Eve is listening in: she hears everything Alice says (but Eve can't see the cards).

   Part A. Suppose Alice's message M is a string of 48-bits. Describe how Alice can communicate M to Bob in such a way that Eve will have *no* information about what is M.

   Part B. Now suppose Alice's message M is 49 bits. Prove that there exists no protocol which allows Alice to communicate M to Bob in such a way that Eve will have no information about M.

   (What does it mean that Eve learns nothing about M? That for all strings κ, the probability that Alice says κ is independent of M: for all messages M_0, M_1 we have that

   $$\Pr[\text{ Alice says } \kappa |\ M = M_0] = \Pr[\text{ Alice says } \kappa |\ M = M_1]\ .$$

   The probability is over the the random shuffle of the cards.)