ECS 227 — Modern Cryptography — Winter 99
Problems 1–4

Phillip Rogaway

Out: 7 January 1999. Due: 21 January 1999.

1. **Composition of EPT Algorithms.** John designs an EPT (expected polynomial time) algorithm to solve some computational problem Π—but he assumes that he has in hand a black-box (ie., a unit-time subroutine) which solves some other computational problem, Π'. Ted soon discovers an EPT algorithm to solve Π'. True or false: putting these two pieces together, John and Ted now have an EPT algorithm for Π. Give a proof or counterexample.

   (When we speak of the worst-case running time of machine M we are looking at the function $T(n)$ which gives, for each n, the maximal time which M might spend on an input of size n: $T(n) = \max_{x,\,|x|=n}[\#\mathrm{Steps}_M(x)]$. When we speak of the expected running time of M we are instead looking at the function $T(n)$ which gives, for each n, the maximal value among inputs of length n of the expected value of the running time of M on this input—that is, $T(n) = \max_{x,\,|x|=n} \mathbf{E}[\#\mathrm{Steps}_M(x)]$, where the expectation is over the random choices made by M.)

2. **Secrecy from a random shuffle.** 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.)

3. **Bijectivity of the function f used in RC6.** Show that the map $x \mapsto x(2x+1) \bmod 2^w$ is one-to-one (and therefore surjective, too) on $\{0, 1, \ldots, 2^w - 1\}$. (In general, $x \mapsto x(rx + s) \bmod 2^w$ is one-to-one on this domain whenever r is even and s is odd. Show this more general statement, if you prefer.)

4. Alternative formulation of real-or-random security (rr2). When I presented our paper on different notions of symmetric encryption at MIT, Ron Rivest raised the following objection to our definition real-or-random security:

> In a chosen-plaintext attack the adversary A should have the ability to obtain the encryptions of messages of her choice. But in your real-or-random definition, the adversary can not do this: she obtains what are either valid encryptions or bogus encryptions — and she can't get, for comparison, what she knows to be valid encryptions. Consider giving the adversary an additional oracle which *always* correctly encrypts. Would this this strengthen your definition?

Answer Rivest's question (being grateful that you have more than 60 seconds to consider this), giving a careful proof. You should begin by introducing any notation you need.