ECS 227 — Modern Cryptography — Spring 07
Problems 1–3

Phillip Rogaway

Out: 11 April 2007. Due: 23 April 2007.

1. **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.)

2. **Alternative formulation of blockcipher security.** Consider the notion of a *strong* PRP: the adversary can query not only E_K-or-π but also the *inverse* permutation E_K^{-1}-or-π^{-1}. Formalize and prove some result that establishes that this notion is *stronger* than our notion of a PRP.

3. **Doubling the blocklength of a blockcipher**. Suppose I give you an $n = 128$ bit blockcipher E that is secure as a PRP. Design a $2n$-bit blockcipher F that you believe will likewise be secure as a PRP. Keep your construction as simple as you can. Explain why F is plausibly a PRP and, if you can, formalize and prove that it is.