Problem Set 6 – Due Wednesday, November 3, at 5pm

1. In class we claimed that S_3, the set of permutations on $\{1, 2, 3\}$, forms a group under composition. Make up a multiplication table for this group. You can name each point in this group in any of the ways we discussed.

2. In cryptography, a **blockcipher** is a function $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ where, for each $K \in \{0,1\}^k$, the function $E(K,\cdot)$ is a permutation on $\{0,1\}^n$. A blockcipher names a collection of permutations $\{E(K,\cdot)\colon\ K \in \{0,1\}^k\}$, one for each $K \in \{0,1\}^k$.

   (a) A common choice for k (the "key size") and n (the "block size") is $k = 256$ and $n = 128$. Under that assumption, what fraction of the permutations on $\{0,1\}^n$ can be named by a blockcipher E? Give a rough numerical estimate. You might find Stirling's formula useful for this. One form of it says that $\lg(n!) \approx n \lg(n) - 1.44n$ where $\lg(x) = \log_2(x)$ is the base-2 logarithm.

   (b) A blockcipher is considered "good" if no "adversary"—no algorithm—can distinguish a black-box that computes $E_K(\cdot)$, for a randomly chosen K, from a black-box that computes $\pi(\cdot)$, for a randomly chosen permutation π from $\text{Perm}(\{0,1\}^n)$. That is, the adversary can ask its black-box any series of questions $X_1, X_2, X_3, \ldots$, to which it gets back answers that are either $E(K, X_1), E(K, X_2), E(K, X_3), \ldots$ or, alternatively, $\pi(X_1), \pi(X_2), \pi(X_3), \ldots$, for a random K or a random π. The adversary aims to distinguish which "kind" of black-box it has. We call it a "black-box" because the adversary's only way to tell what kind of black-box it has is to study the responses to queries.

   Is there any "philosophical" difficulty concerning the existence of a "good" blockcipher with parameters $k = 256$ and $n = 128$? (Hint: concerns arise as soon as the adversary asks *three* questions.) Can you think of a way that one might try to get around this problem without changing k or n?

3. Use the relative sizes of infinites sets to show that computers cannot decide (that is, answer the membership question) *most* languages.