Problem Set 1

Due at the *beginning* of class on Sept. 21

1. In each of the following cases, write the given expression in your own words (in English, not equations) and determine its value.

   (a) $\Pr[x \leftarrow \{0,1\}^4 : x = 0100]$.

   (b) $\Pr[x \leftarrow \{0,1\}^{10}; y \leftarrow \{0,1\}^{10} : x = y]$.

   (c) Let A be an algorithm such that $A(x)$ outputs 1 if and only if the first three bits of x are 0, let $(\mathcal{E}, \mathcal{D})$ denote the one-time pad encryption scheme, and consider the following two expressions:

   $$\Pr\left[k \leftarrow \{0,1\}^{\ell}; C \leftarrow \mathcal{E}_k(0^{\ell}) : A(C) = 1\right]$$
   $$\Pr\left[k \leftarrow \{0,1\}^{\ell}; C \leftarrow \mathcal{E}_k(1^{\ell}) : A(C) = 1\right].$$

2. In class we discussed *perfect secrecy* for the case when the adversary sees the encryption of a single message; we also showed the one-time pad scheme and said that it was secure only in this case.

   (a) Formulate a definition of perfect secrecy for the case when the adversary sees the encryption of *two* messages (using the same key). Your definition may be modeled on any of the three definitions of perfect secrecy given in class.

   (b) Does there exist a *deterministic* encryption scheme with perfect secrecy under your definition in part (a)? Does it help if we allow encryption to be *randomized*? Prove or disprove your assertion in each case.

   (c) If the answer to part (b) is "no" for the case of deterministic encryption, suggest an alternate definition of perfect secrecy when two messages are encrypted which might be achievable by a deterministic scheme. (You do not need to construct such a scheme, but will get extra credit if you do so for a suitable alternate definition!)

3. Another definition of security that is sometimes (mistakenly) considered for private-key encryption is *security against key-recovery attacks*. Consider the following definition of this notion:

   > An encryption scheme $(\mathcal{E}, \mathcal{D})$ with associated key space $\mathcal{K}$ and message space $\mathcal{M}$ is *perfectly-secure against key recovery* if the following holds for any algorithm A and any distribution Dist over the message space $\mathcal{M}$:
   >
   > $$\Pr[k \leftarrow \mathcal{K}; m \leftarrow \mathsf{Dist}; C \leftarrow \mathcal{E}_k(m) : A(C) = k] \leq \frac{1}{|\mathcal{K}|}.$$

Answer the following questions:

(a) Explain the above definition in your own words.

(b) Show that the above definition is not *necessary* for perfectly-secure encryption. I.e., show that there exists an encryption scheme which is perfectly-secure under the definition we gave in class, but not perfectly-secure against key recovery.

(c) Show that the above definition is not *sufficient* for perfectly-secure encryption. I.e., show that there exists an encryption scheme which is perfectly-secure against key recovery, but not perfectly-secure under the definition we gave in class.

4. Recall the definition of a *one-way function* given in class. Let f and g be one-way functions. The notation "$\circ$" denotes string concatenation.

   (a) Consider the function f' defined as $f'(x_1 \circ x_2) = f(x_1) \circ x_2$ (where $|x_1| = |x_2|$). Prove or disprove whether f' is a one-way function. (I.e., is f' a one-way function for *every* one-way function f?)

   (b) Consider the function g' defined as $g'(x_1 \circ x_2) = x_1 \circ g(x_2)$ (where $|x_1| = |x_2|$). Prove or disprove whether g' is a one-way function. (I.e., is g' a one-way function for *every* one-way function g?)

   (c) Consider the function h defined as $h(x) = f(x) \circ g(x)$. Prove or disprove whether h is a one-way function. (I.e., is h a one-way function for *all* one-way functions f, g?)