University of Maryland
CMSC858K — Cryptography
Professor Jonathan Katz

Problem Set 1

Due at *beginning* of class on Feb. 20

1. **(Perfect secrecy.)** In class we gave three different definitions of perfect secrecy over message space $\mathcal{M}$:

   (a) An encryption scheme is perfectly secret if for all probability distributions over $\mathcal{M}$, for any $m \in \mathcal{M}$, and for all ciphertexts C we have:

   $$\Pr[m|C] = \Pr[m].$$

   (b) An encryption scheme is perfectly secret if the following holds for all $m_1, m_2 \in \mathcal{M}$: Let the *a priori* distribution over $\{m_1, m_2\}$ be the uniform distribution. Then for all ciphertexts C we have:

   $$\Pr[m_1|C] = \Pr[m_2|C].$$

   (c) An encryption scheme is perfect secret if, for all $m_1, m_2 \in \mathcal{M}$ and for any adversary A we have:

   $$\Pr[k \leftarrow \mathcal{K}; C \leftarrow \mathcal{E}_k(m_1) : A(C) = 1] = \Pr[k \leftarrow \mathcal{K}; C \leftarrow \mathcal{E}_k(m_2) : A(C) = 1].$$

   Show that these definitions are all equivalent.

2. **(Negligible functions.)** Let $\epsilon : \mathbb{N} \to \mathbb{R}^+$ be a negligible function. Prove that each of the following functions are also negligible.

   (a) $\epsilon'(k) \stackrel{\text{def}}{=} p(k) \cdot \epsilon(k)$, where $p(k) = O(k^c)$ ($c \geq 0$ is any constant). (I.e., $p(k)$ is upper-bounded by some polynomial.)

   (b) $\epsilon''(k) \stackrel{\text{def}}{=} \epsilon(\nu(k))$, where $\nu(k) = \Omega(k^c)$ ($c > 0$ is any constant). (I.e., $\nu(k)$ is at least polynomial in k.)

3. **(PRGs imply OWFs.)** Prove that if a length-doubling pseudorandom generator exists, then one-way functions exist. (Your proof should be direct, and not via private-key encryption.)

4. **(One-way functions.)** For any binary string x, let x_i denote the i^{th} bit of x. Let $F = \{f_k : \{0,1\}^k \to \{0,1\}^k\}_{k \geq 1}$ be a one-way function family. Define $F' = \{f'_k : \{0,1\}^k \to \{0,1\}^k\}_{k \geq 1}$ via $f'_k(x) \stackrel{\text{def}}{=} f_{k-1}(x_1 \cdots x_{k-1}) \circ x_k$, where $\circ$ is just concatenation. Show that F' is a one-way function family.

5. **(Extra credit — non-existence of "direct" hard-core bits.)** In this problem, we construct a one-way function in which each bit of the pre-image is "easy" to predict (namely, can be predicted with probability 3/4). This shows why extracting hard-core bits from one-way functions is very difficult in general! Let F be as in the previous problem. Define functions $c : \{0,1\}^3 \to \{0,1\}$ and $d : \{0,1\}^3 \to \{0,1\}^2$ as follows:

x	c(x)	d(x)
000	0	00
001	0	01
010	0	10
100	0	11
011	1	00
101	1	01
110	1	10
111	1	11

Furthermore, for any integer $k > 1$ and any $x \in \{0,1\}^{3k}$, define:

$$\hat{c}(x) \stackrel{\text{def}}{=} c(x_1x_2x_3) \circ c(x_4x_5x_6) \circ \cdots \circ c(x_{3k-2}x_{3k-1}x_{3k})$$
$$\hat{d}(x) \stackrel{\text{def}}{=} d(x_1x_2x_3) \circ d(x_4x_5x_6) \circ \cdots \circ d(x_{3k-2}x_{3k-1}x_{3k}).$$

Finally, define $G = \{g_k : \{0,1\}^{3k} \to \{0,1\}^{3k}\}_{k \geq 1}$ via:

$$g_k(x) \stackrel{\text{def}}{=} \hat{c}(x) \circ f_{2k}(\hat{d}(x)).$$

(a) If f_{2k} is a permutation, is g_k a permutation?

(b) Assume f_k is always a permutation. Show that given $g_k(x)$, any individual bit of x can be guessed correctlly with probability 3/4. (*Hint:* use the information given to you by $\hat{c}(x)$.)

(c) Show that G is a one-way function family. (*Hint:* Given an algorithm inverting g_k, construct an algorithm inverting f_{2k}. Use the fact that the value $c(x)$ is uncorrelated with the value $d(x)$.)