CAS CS 538. Problem Set 3

Due in class Tuesday, September 25, 2012, *before* the start of lecture

Problem 1. (30 points) In the first week, we showed that if a cryptosystem is Shannon secure, then $|K| \geq |M|$. However, perfect security is a very strong condition: it requires than for any $m_0, m_1 \in M$, $\Delta(\text{Enc}_k(m_0), \text{Enc}_k(m_1)) = 0$. (Note that each of these two random variables is produced by taking a uniform key $k \in K$ and then applying the encryption function.) Given what we now know about statistical distance, we could relax this requirement, replacing 0 with some small value ϵ. This would imply that Eve cannnot distinguish the encryption of m_0 from the encryption of m_1 with advantage greater than ϵ, even if she has unlimited computational powers. In this problem, you will show that this particular relaxation does not help shrink the key space much.

(a) (10 points) Let $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ be random variables. Let X (respectively, Y) be the random variable produced by picking i uniformly at random between 1 and n and then choosing the value of X_i (respectively, Y_i). That is, $\Pr[X = x] = \frac{1}{n} \sum_{i=1}^{n} \Pr[X_i = x]$, and similarly for Y. Prove that $\Delta(X, Y) \leq \frac{1}{n} \sum_{i=1}^{n} \Delta(X_i, Y_i)$.

(b) (10 points) Suppose that, for a given cryptosystem and for all m_0, $m_1 \in M$,

$$\Delta(\text{Enc}_k(m_0), \text{Enc}_k(m_1)) \leq \epsilon\,.$$

Let m denote the uniform distribution on the set M. Show that for all m_0,

$$\Delta\left((m, \text{Enc}_k(m_0)), (m, \text{Enc}_k(m))\right) \leq \epsilon$$

(note that the last two occurrences of m refer to the same value). In other words, one random variable contains a random message and an encryption of m_0, and the other contains a random messages and its encryption. (Hint: use problem 2 (specifically, item 5 of Lemma 6.3) from PS2 to show that $\Delta((m_1, \text{Enc}_k(m_0)), (m_1, \text{Enc}_k(m_1))) \leq \epsilon$; then apply the previous part to average over all m_1).

(c) (10 points) Finally, show that if for all $m_0, m_1 \in M$, $\Delta(\text{Enc}_k(m_0), \text{Enc}_k(m_1)) \leq \epsilon$, then $|K| \geq |M|(1 - \epsilon)$. (Hint: use the previous part; if the key space is too small, then it's unlikely that any key will decrypt an encryption of m_0 to a random m; this observations gives you a distinguisher).

Note: The answers below must be *proven* using one of the two definitions of pseudorandomness used in class.

Problem 2. (40 points)

(a) (20 points)
Suppose an algorithm G is a pseudorandom generator. Let $\bar{G}$ be the following algorithm: on input seed s, run $G(s)$ to get w, then negate every bit of w to get $\bar{w}$ (i.e., for bit i, $\bar{w}_i = 1 - w_i$), and output the result. Prove by using a reduction that $\bar{G}$ is also a pseudorandom generator.

(b) (20 points)
Suppose algorithms G_1 and G_2 are pseudorandom generators. Let G_3 be the following algorithm: on input s, G_3 runs $G_1(s)$ to get w_1, runs $G_2(s)$ to get w_2, and ouptuts the concatenation of the two

strings: $w_3 = w_1 \circ w_2$. Show that G_3 is *not* necessarily a pseudo-random generator. (Hint: it may be helpful to use what you proved in the previous part.)

Problem 3. (30 points)
In the previous problem, we saw an *insecure* way to combine two pseudorandom generators: run them on the same seed. Here we will show that running them on two *independent* seeds is *secure*.

Suppose algorithms G_1 and G_2 are pseudorandom generators. Let G_3 be the following algorithm: on input s_3 (assume length of s_3 is even), G_3 splits s_3 in half to get two strings s_1 and s_2 of half the length. Then G_3 runs $G_1(s_1)$ to get w_1, runs $G_2(s_2)$ to get w_2, and ouptuts the concatenation of the two strings: $w_3 = w_1 \circ w_2$. Show G_3 is a pseudorandom generator. (Hint: suppose it's not. Then there is a distinguisher that can tell w_3 from random. Use a "hybrid" argument—unlike the complicated one we did in class, where we had many intermediate points, here you only need one intermediate point.)