Problem Set 2

Due: Thursday 10/16/2014, by 11:00am

1. Recall the definition of experiment $\text{Priv}_{A,\Pi}^{\text{adv}}$. Let $\Pi$ denote the Vignère cipher where the message space consists of all 3-character strings over the lowercase English alphabet, and the key is generated by first choosing the period $t$ uniformly from $\{1, 2, 3\}$ and then letting the key be a uniform string of length $t$.

   (a) Define $A$ as follows: $A$ outputs $\{m_0 = \text{aad}, m_1 = \text{adp}\}$. When it is given the challenge ciphertext $c$, it outputs 0 if the first character of $c$ is the same as the second character of $c$, and outputs 1 otherwise. Compute $\text{Prob}[\text{Priv}_{A,\Pi}^{\text{adv}} = 1]$.

   (b) Describe and analyze an adversary $A'$ for which $\text{Prob}[\text{Priv}_{A',\Pi}^{\text{adv}} = 1]$ is greater than your answer from part (a).

2. Write a program that increments a counter $2^{24}, 2^{25}, 2^{26}, \ldots, 2^{33}$ times, and measure how many seconds your program takes to run in each case. Estimate how many years your program would take to increment a counter $2^{64}$ or $2^{128}$ times.

3. Let $G : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be a PRG. For each of the following constructions, prove whether it is necessarily a PRG or not. (Each of these constructions starts by parsing the input as two equal-length parts).

   (a) $G_1(s, t) = G(s) \parallel t$ where $|s| = |t|$.

   (b) $G_2(s, t) = G(s, t) \parallel t$ where $|s| = |t|$.

4. Problem 3.10 in textbook (proving that $F_k(x) = G'(k) \oplus x$ is not a PRF).

5. Let $F'$ be a PRF that for an $n$-bit key and an $n$-bit input gives a $2n$-bit output. Define a new keyed function $F$ (or a family of functions $\{F_k\}$) as follows.

   $\forall x, F_{0^n}(x) = 0^{2n}$ (constant 0 function), and $F_k(x) = F'_k(x)$ for $k \neq 0^n$.

   (a) Prove that if $F'$ is a PRF, then $F$ is also a PRF.

   (b) Prove that the candidate construction $G(s) = F_{0^n}(s)$ is not a PRG.

6. Let $F$ be a PRF and $G$ a PRG. Below we describe some private-key encryption schemes (the key generation algorithm always chooses a uniformly random string $k \in \{0, 1\}^n$, and we omit the message space and the decryption algorithm, but check that you can figure out what these are). For each of these encryption schemes state whether the scheme is EAV-secure (one time ciphertext only attack), and whether it is CPA secure. Provide a brief informal justification (a formal proof is not necessary).

   (a) To encrypt $m$, output $F_k(0) \oplus m$.

   (b) Choose a random $r$ and output $(r, G(r) \oplus m)$

   (c) Choose a random $r$ and output $(r, F_r(k) \oplus m)$.

   (d) Choose a random $r$ and output $(r, F_k(r \oplus m))$. 