University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Homework 2

Due at the *beginning* of class on Oct. 2

1. Exercise 2.2.

2. Exercise 2.3.

3. Exercise 2.4.

4. Exercise 2.9.

5. Recall the definition of experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$. Let Π denote the Vigenère 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 $\mathcal{A}$ as follows: $\mathcal{A}$ outputs $\{m_0 = \texttt{aab},\ m_1 = \texttt{abb}\}$. When it is given a ciphertext c, it outputs '0' if the first character of c is the same as the second character of c, and '1' otherwise. Compute $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1]$.

   (b) Give pseudocode for an adversary $\mathcal{A}'$ for which $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A}',\Pi} = 1]$ is greater than your answer from part (a).

6. 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.

7. Available online is a program, `prg.c`, that implements a simple PRG with expansion factor $n+8$ as well as a simple "testing harness" that computes the distinguishing advantage

$$\left|\Pr[D(r)=1] - \Pr[D(G(s))=1]\right|$$

   (for r a uniform $(n+8)$-bit string, and s a uniform n-bit string) for a distinguisher D that you specify. (1) Write code for a distinguisher D whose distinguishing advantage is at least 0.5; also (2) analyze mathematically what distinguishing advantage you expect for your distinguisher. Your distinguisher should run in time *polynomial* in `SEC_PARAM`.