University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Homework 2

Due at the *beginning* of class on Sept. 19

1. Exercise 2.5.
2. Exercise 2.7. (Feel free to ignore the hint.)
3. Exercise 2.8.
4. Exercise 2.9.
5. Recall the definition of experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ (see page 34). Let Π denote the Vigenère cipher where the message space consists of all 3-character strings over the 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 $\{m_0 = \mathtt{aab},\ m_1 = \mathtt{abb}\}$. 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) Construct and analyze an adversary $\mathcal{A}'$ for which $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A}',\Pi} = 1]$ is greater than your answer from part (a).
6. Exercise 3.2.
7. Exercise 3.6. (Assume $|G(s)| > 2 \cdot |s|$.)