University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 1

Due at the *beginning* of class on Sept. 12

1. Write a program that performs cryptanalysis of ciphertexts encrypted using the Vigenere cipher. As outlined in the text, your program should operate in the following steps:

   (a) First determine the length of the key (i.e., the period) using the index of coincidence method. You may assume that the key has length at most 6.

   (b) Next, use the "improved" method for attacking the shift cipher to completely determine the plaintext.

   Use your program to recover the plaintext corresponding to a ciphertext that can be downloaded from the course homepage. (Linebreaks were inserted just for convenience.) Hand in a printout of your program in addition to your solution.

2. An encryption scheme is formally defined by algorithms Gen, Enc, and Dec, as well as a message space $\mathcal{M}$. Give formal specifications of these components for the shift cipher, the substitution cipher, and the Vigenere cipher (for the latter, you may assume the key always has length 5).

3. A randomized algorithm A taking k inputs $x_1, \ldots, x_k$ can be viewed as a deterministic algorithm taking $k+1$ inputs $x_1, \ldots, x_k, r$, where the (randomized) output of $A(x_1, \ldots, x_k)$ is determined by choosing a sufficiently-long random string r and then outputting the (deterministic) value $A(x_1, \ldots, x_k; r)$. (In this case, r is called the *random coins* used by A, and we distinguish it from other inputs by using a semicolon instead of a comma.)

   Prove that, in the context of private-key encryption, we can assume without loss of generality that keys are chosen uniformly at random (and so Gen is trivial). I.e., show that for any encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ (over any message space), there is a functionally equivalent encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where Gen simply outputs its random coins. (I am looking for formal specifications of Enc and Dec.)