University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

Homework 1
Due at the *beginning* of class on Feb. 8

 All numbered exercises refer to the second edition of the book.

1. (Exercise 1.3.)
   Provide formal definitions of the Gen, Enc, and Dec algorithms for the Vigenère cipher.
   (Note: there are several plausible choices for Gen; choose one.)

2. (Exercise 1.5.)
   Show that the shift, substitution, and Vigenère ciphers are all trivial to break under
   a chosen-plaintext attack. How much chosen-plaintext is needed to recover the key in
   each case?

3. (Exercise 1.6.)
   Assume an attacker knows that a user's password is either `abcd` or `bedg`. Say the
   user encrypts her password using the shift cipher, and the attacker sees the resulting
   ciphertext. Show how the attacker can determine the user's password, or explain why
   this is not possible.

4. (Exercise 1.7.)
   Repeat the previous exercise for the Vigenère cipher using period 2, period 3, and
   period 4.

5. Decrypt the ciphertext available online that was generated using the Vigenère ci-
   pher. (C code for encryption/decryption is provided as well.) Note that you may use
   lowercase letter frequencies or ASCII character frequencies to solve this problem.

   Hand in the solution (i.e., the decrypted plaintext) as well as a printout of the source
   code you wrote to recover it. You can use any programming language of your choice.