University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

# Homework 1

**Due at the *beginning* of class on Sept. 18**

1. Exercise 1.2.
2. Exercise 1.6. (You don't need to compare to the previous question.)
3. Assume a user's password is either `abad` or `acae`. Say the user encrypts his password using the shift cipher, and an attacker sees the resulting ciphertext. Show how the attacker can determine the user's password, or explain why this is not possible.
4. Repeat the previous question for the Vigenère cipher using period 2.
5. Decrypt the ciphertext available online that was generated using the Vigenère cipher. (C code for encryption/decryption—but not the period or the key!—is provided as well.) Note: the intent of this question is for you to explore the algorithm for attacking the Vigenère cipher. This question is *not* intended to be a test of your low-level programming abilities, so do not hesitate to ask questions about such things on Piazza.

   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.