Introduction to Cryptology ENEE459E/CMSC498R: Homework 1

Due by beginning of class on 2/6/2019.

1. Cracking the Vigenere cipher. Use the cryptanalysis methods discussed in class to decrypt the ciphertext available on the course webpage that was generated using the Vigenere cipher. Your solution should include the recovered secret key and plaintext as well as a printout of the code you used. You may use the programming language of your choice. **You may assume that the key length is at most 10.**

2. Provide a formal definition of the Gen, Enc, and Dec algorithms for the mono-alphabetic substitution cipher.

3. Show that the shift, substitution, and Vigenere ciphers are all trivial to break using a known-plaintext attack. How much known plaintext is needed to recover the key for each of the ciphers? (Make your assumptions explicit.) Repeat this exercise for a chosen-plaintext attack.

   Some background information (see also pages 19-20 of textbook): In a **known plaintext attack**, the adversary Eve is allowed additional information. As before, the secret key k is chosen by running Gen, a message m is drawn from the message distribution and a ciphertext $c \leftarrow \mathsf{Enc}_k(m)$ is computed. But now, Eve gets to observe the ciphertext c and additionally learn the corresponding plaintext m. In a **chosen plaintext attack**, Eve gets to specify the message m to be encrypted and then observes $c \leftarrow \mathsf{Enc}_k(m)$.

4. Assume an attacker knows that a users password is either abcd or bedg. Say the user encrypts his password using the shift cipher, and the attacker sees the resulting ciphertext. Show how the attacker can determine the users password, or explain why this is not possible.