# Introduction to Cryptology ENEE459E/CMSC498R: Homework 1

Due by beginning of class on 2/18/2014.

1. **Cracking the Vigenere cipher.** Use the cryptanalysis methods discussed in class to decrypt the ciphertext available online that was generated using the Vigenere cipher.

2. Exercises 1.5, 1.6.

   Some background information (see also pages 8-9 of textbook): In a **known plaintext attack**, the adversary Eve is allowed additional information. As before, the secret key $k$ is chosen by running $\mathsf{Gen}$, 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 $c \leftarrow \mathsf{Enc}_k(m)$.

3. Prove that Definition 2.4 is equivalent to Definition 2.1 (Exercises 2.7, 2.8)

4. Exercise 2.2

5. Exercise 2.10

6. For each of the following encryption schemes, state whether the scheme achieves perfect secrecy. Justify your answer using Definitions 2.1 and/or Lemmas 2.2, 2.3.

   (a) Message space $\mathcal{M} = \{0, 1, \ldots, n-1\}$. Key space $\mathcal{K} = \{0, 1, \ldots, n-1\}$. $\mathsf{Gen}()$ chooses a key $k$ at random from $\mathcal{K}$. $\mathsf{Enc}_k(m)$ returns $m + k$. $\mathsf{Dec}_k(c)$ returns $c - k$.

   (b) Message space $\mathcal{M} = \{0, 1, \ldots, n-1\}$. Key space $\mathcal{K} = \{0, 1, \ldots, n-1\}$. $\mathsf{Gen}()$ chooses a key $k$ at random from $\mathcal{K}$. $\mathsf{Enc}_k(m)$ returns $(m + k) \mod n$. $\mathsf{Dec}_k(c)$ returns $(c - k) \mod n$.

   (c) Message space $\mathcal{M} = \{0,1\}^{2n}$. Key space $\mathcal{K} = \{0,1\}^{2n}$. $\mathsf{Gen}()$ chooses $k_1, k_2$ at random from $\{0,1\}^n$. $\mathsf{Enc}_{k_1||k_2}(m_1||m_2)$ returns $m_1 \oplus k_1 || m_2 \oplus (k_1 \oplus k_2)$. $\mathsf{Dec}_{k_1||k_2}(c_1||c_2)$ returns $c_1 \oplus k_1 || c_2 \oplus (k_1 \oplus k_2)$.

   (d) Message space $\mathcal{M} = \{1, \ldots, p-1\}$. Key space $\mathcal{K} = \{1, \ldots, p-1\}$, for prime $p$. $\mathsf{Gen}()$ chooses a key $k$ at random from $\mathcal{K}$. Let $k'$ be such that $k \cdot k' \equiv 1 \mod p$. $\mathsf{Enc}_k(m)$ returns $m \cdot k \mod p$. $\mathsf{Dec}_k(c)$ returns $c \cdot k' \mod p$.

   (e) What happens when $p$ is not prime?