University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

Problem Set 1

This is an ungraded homework, intended to make you think further about some of the concepts covered in class.

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

1. Exercise 1.3.

2. Exercise 1.6.

3. Exercise 1.7.

4. Consider the *double (ASCII) Vigenère cipher*, where we choose two keys (possibly of different lengths) k_1, k_2, and then encrypt a message by encrypting it first using the ASCII Vigenère cipher with k_1 to obtain an intermediate ciphertext c', and then encrypting c' using the ASCII Vigenère cipher with k_2 to obtain the final ciphertext c. How would you attack this scheme?

5. We talked about attacking the ASCII Vigenère cipher in two steps:

   - First find the key length in the following way: for each candidate length $\ell = 1, \ldots,$ compute the frequencies $\{q_i\}_{i=0}^{255}$ of the characters in a "stream" of the ciphertext consisting of characters separated by distance ℓ; then choose ℓ for which $\sum q_i^2$ is maximized.
   - Say the key length is L. Next, find each byte of the key as follows: let $\{q_i\}_{i=0}^{255}$ be the frequencies of the characters in a "stream" of the ciphertext. Then for a particular guess B for that byte, compute $I_B = \sum q_{i \oplus B} \cdot p_i$, where the $\{p_i\}$ are the frequencies of ASCII characters in normal English text (assume those values are known).

   What happens if both the above steps are executed, but the underlying plaintext was written in a language other than English?