University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Homework 1

Due at the *beginning* of class on Sept. 20

1. Write a program (in any language) that performs cryptanalysis of ciphertexts encrypted using the Vigenère cipher using the method described in class (and in the book). Use your program to recover the plaintext corresponding to a ciphertext that can be downloaded from the course homepage. (Linebreaks were inserted just for convenience; make sure to ignore them in your attack.) Hand in a printout of your program in addition to the plaintext.

2. An encryption scheme is formally defined by algorithms Gen, Enc, and Dec, as well as a message space $\mathcal{M}$. Give formal specifications for the shift cipher, the substitution cipher, and the Vigenère cipher (for the latter, assume the key always has length 5).

3. (Exercise 1.3.) The Vigenère cipher can be viewed as a generalization of the shift cipher. Consider the following analogous generalization of the substitution cipher: The key consists of t random permutations of the alphabet $\pi_1, \ldots, \pi_t$, and the plaintext characters in positions $i, t+i, 2t+i, \ldots$ are encrypted using π_i. (E.g., if $t = 3$ then the encryption of 'abcdef' would be $\pi_1(a), \pi_2(b), \pi_3(c), \pi_1(d), \pi_2(e), \pi_3(f)$.) Describe a ciphertext-only attack that recovers the plaintext. (Treat t as unknown, but you can assume a known upper bound on t.)

4. (Exercise 2.3.) When using the one-time pad encryption scheme, it can occur that $k = 0^\ell$ and then the ciphertext is equal to the plaintext! It has been suggested to improve the one-time pad by only choosing *non-zero* keys. What do you think of this improvement? In particular, is it still perfectly secret? If yes, prove it. If no, reconcile this with the fact that encryption with the all-0 key completely reveals the plaintext.

5. (Exercise 2.4.) In this exercise, we study conditions under which the shift, mono-alphabetic substitution, and Vigenére ciphers are perfectly secret:

   (a) Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.

   (b) What is the largest plaintext space $\mathcal{M}$ you can find for which the mono-alphabetic substitution cipher provides perfect secrecy? (Note: $\mathcal{M}$ need not contain only valid English words.)

   (c) Show how to use the Vigenére cipher to encrypt any word of length t so that perfect secrecy is obtained (note: you can choose the length of the key). Prove your answer.

   Reconcile the above claims of perfect secrecy with the ciphertext-only attacks on these ciphers that were shown in class.