MATH/CSCI 4116: CRYPTOGRAPHY, FALL 2014

Handout 1

Personalized for: XXXXXXXXXXXXX

Homework 2, due Sep 24:

Problem 1. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with an affine cipher. Explain your method.

(see personalized handout)

Problem 2. Use a "ciphertext only" attack to decrypt the following text. It has been encrypted with a Vigenere cipher. Explain your method.

(see personalized handout)

Problem 3. Consider the following variant of a shift cipher: instead of shifting each letter by the same amount, we shift each letter by a different amount. The key consists of two integers n and m, and to encrypt, we shift the ith letter by $n + im$ places in the alphabet. In other words, if p_i is the ith plaintext letter, and c_i is the ith ciphertext letter, then the encryption rule is:

$$c_i \equiv p_i + n + im \pmod{26}$$

Let's count letters from 0, so that p_0 is the first plaintext letter, p_1 is the second plaintext letter, and so forth.

(a) Encrypt "mathematics" using $n = 2$, $m = 3$.

(b) Decrypt "hvvahivknzhfqhl" using $n = 5$, $m = 2$.

(c) Discuss the relative strength of this cipher under the four different attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.

(d) Can you launch a successful "ciphertext only" attack on the following message?

(see personalized handout)

Note: the above ciphertexts are also available from:
`http://www.mathstat.dal.ca/~selinger/4116/ciphertexts.txt`.