CS 435: Introduction to Cryptography **2012 Fall**

Solutions 1

Professor Somesh Jha

1. Both Kasiski's attack and the index of coincidence method can be used to recover the key length in this version of the Vigenère cipher, just as in the original. After the key length t is known, each of the t monoalphabetic substitutions can be broken with letter frequency analysis.

2. (a) Using a known-plaintext attack, each cipher can be broken as follows:
   - Subtract the first letter of the known plaintext from its corresponding ciphertext; this will give the value of the shift. Only a single letter is needed to completely recover the key.
   - Given a plaintext m and its corresponding ciphertext c, we know that the i-th character m_i of m encrypts to the i-th character c_i of c. To completely recover the key, we need m to contain at least 25 of the 26 letters of the alphabet.
   - Given a plaintext m and its corresponding ciphertext c, we can subtract the i-th character m_i of the plaintext from the i-th character c_i of the corresponding ciphertext to obtain the value of the shift at that position. By noting when these values start to repeat, we can get the length of the key. Assuming the key has a length of t, a plaintext m of length at least t is needed to completely recover the key.

   (b) Same as (a), except we choose plaintexts that satisfy the minimum requirements set forth there, e.g. `a` for the shift cipher, `abc...xy` for the monoalphabetic substitution cipher, and any string of length at least t for the Vigenère cipher.

3. Since each plaintext character m_i maps to each of its associated ciphertext characters c_i and c_i' with equal probability, the peaks of c_i and c_i' will have similar heights on the frequency histogram. One possible attack involves matching pairs of ciphertext characters with similar frequencies, assuming they correspond to the same plaintext character, and carrying out a letter frequency analysis as in the original attack on the monoalphabetic substitution cipher.

4. Since we know the plaintext is either `vegetarians` or `bacongrease`, we can calculate what the key would be in each of these cases by subtracting the i-th character m_i of the plaintext from the i-th character c_i of the ciphertext, and taking the result modulo 26. Since the encryption scheme requires the key to be intelligible, we can determine which key was used by observing which one appears to be in English.

   If the message is `vegetarians`, then the key must be `ohkfyyoiext`, while if the message was `bacongrease`, the key is `ilovesomesh`. Since `ilovesomesh` is an English-language phrase and `ohkfyyoiext` isn't, the plaintext is `bacongrease`.