密碼學與應用作業

94/10/13 (四)

1. Suppose the plaintext alphabets include a~z, A~Z, 0~9, and the space character, therefore, we work on 63 instead of 26 for an affine cipher. How many keys are possible? What if we add ‘;’, ‘.’, ‘,’, and ‘?’ characters to our plaintext alphabet set, i.e. we work on 67 instead?

2. The ciphertext UJVDDP was encrypted by a Hill cipher with matrix $\begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}$.

   Find the corresponding plaintext.

3. (Trappe 2nd Ed. Chap3.18) Let a, b, c, d, e, f be integers mod 26. Consider the following combination of the Hill and affine ciphers: Represent a block of plaintext as a pair (x, y) mod 26. The corresponding ciphertext (u, v) is

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \end{pmatrix} \equiv \begin{pmatrix} u & v \end{pmatrix} \pmod{26}$$

   Describe how to carry out a chosen plaintext attack on this system (with the goal of finding the key a, b, c, d, e, f). You should state explicitly what plaintexts you choose and how to recover the key.

4. (Trappe 2nd Ed. Chap3.20) Consider the sequence starting as $k_1=1$, $k_2=0$, $k_3=1$ and define by the length-three recurrence $k_{n+3} = k_n + k_{n+1} + k_{n+2}$. This sequence can also be given by a length-two recurrence. Determine this length-three recurrence by setting up and solving the appropriate matrix equations. Briefly explain the reason why it can be defined by a length-two recurrence equation. Is there a condition such that every sequence satisfying this condidtion has a unique recurrence describing it?

5. (Trappe 2nd Ed. Chap3.25) The operator of a Vigenere encryption machine is bored and encrypts a plaintext consisting of the same letter of the alphabet repeated several hundred times. The key is a six-letter English word. Eve knows that the key is a word but does not yet know its length.

   (a) What property of the ciphertext will make Eve suspect that the plaintext is one repeated letter and will allow her to guess that the key length is six?

   (b) Once Eve recognizes that the plaintext is one repeated letter, how can she determine the key? (Hint: You need the fact that no English word of length six is a shift of another English word.)

(c) Suppose Eve doesn’t notice the property needed in part (a), and therefore uses the method of displacing then counting matches for finding the length of the key. What will the number of matches be for the various displacements? In other words, why will the length of the key become very obvious by this method?