Applied Cryptography: Homework 3

(Deadline: 10:00am, 2020/09/30)

Justify your answers with calculations, proofs, and programs.

1. (20 points, question 2.25, page 56 of the textbook)

   Here is how we might cryptanalyze the *Hill Cipher* using a ciphertext-only attack. Suppose that we know that $m = 2$. Break the ciphertext into blocks of length two letters (digrams). Each such digram is the encryption of a plaintext digram using the unknown encryption matrix. Pick out the most frequent ciphertext digram and assume it is the encryption of a common digram in the list following Table 2.1 in the textbook (for example, *TH* or *ST*). For each such guess, proceed as in the known-plaintext attack, until the correct encryption matrix is found.

   Here is a sample of ciphertext for you to decrypt using this method:

   ```
   LMQETXYEAGTXCTUIEWNCTXLZEWUAISPZYVAPEWLMGQWYA
   XFTCJMSQCADAGTXLMDXNXSNPJQSYVAPRIQSMHNOCVAXFV
   ```

2. (10 points, question 3.3, page 80 of the textbook)

   Let n be a positive integer. A **Latin square** of order n is an $n \times n$ array L of the integers $1, \ldots, n$ such that every one of the n integers occurs exactly once in each row and each column of L. An example of a Latin square of order 3 is as follows:

1	2	3
3	1	2
2	3	1

   .

   Given any Latin square L of order n, we can define a related *Latin Square Cryptosystem*. Take $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, \ldots, n\}$. For $1 \leq i \leq n$, the encryption rule e_i is defined to be $e_i(j) = L(i, j)$. (Hence each row of L gives rise to one encryption rule.)

   Give a complete proof that this *Latin Square Cryptosystem* achieves perfect secrecy provided that every key is used with equal probability.

3. (20 points, question 3.4, page 80 of the textbook)

   Let $\mathcal{P} = \{a, b\}$, and let $\mathcal{K} = \{K_1, K_2, K_3, K_4, K_5\}$. Let $\mathcal{C} = \{1, 2, 3, 4, 5\}$, and suppose the encryption functions are represented by the following encryption matrix:

	a	b
K_1	1	2
K_2	2	3
K_3	3	1
K_4	4	5
K_5	5	4

   .

   Now choose two positive real numbers α and β such that $\alpha + \beta = 1$, and define $\Pr[K_1] = \Pr[K_2] = \Pr[K_3] = \alpha/3$ and $\Pr[K_4] = \Pr[K_5] = \beta/2$.

   Prove that this cryptosystem achieves perfect secrecy.

4. (10 points, question 3.9, page 81 of the textbook)

   (a) Construct the encryption matrix (as defined in Example 3.3) for the *One-time Pad* with $n = 3$.

   (b) For any positive integer n, give a direct proof that the encryption matrix of a *One-time Pad* defined over $(\mathbb{Z}_2)^n$ is a Latin square of order 2^n, in which the symbols are the elements of $(\mathbb{Z}_2)^n$.