Applied Cryptography: Homework 3

(Deadline: 3:00pm, 2022/03/09)

Justify your answers with calculations, proofs, and programs.

1. (10 points, question 2.23, page 55 of the textbook) Suppose we are told that the plaintext

   breathtaking

   yields the ciphertext

   RUPOTENTOIFV

   where the *Hill Cipher* is used (but m is not specified). Determine the encryption matrix.

2. (10 points, question 2.30, page 58 of the textbook) We describe another stream cipher, which incorporates one of the ideas from the Enigma machime used by Germany in World War II. Suppose that π is a fixed permutation of $\mathbb{Z}_{26}$. The key is an element $K \in \mathbb{Z}_{26}$. For all integers $i \geq 1$, the keystream element $z_i \in \mathbb{Z}_{26}$ is defined according to the rule $z_i = (K + i - 1) \mod 26$. Encryption and decryption are performed using the permutations π and π^{-1}, respectively, as follows:

   $$e_z(x) = \pi(x) + z \mod 26$$

   and

   $$d_z(y) = \pi^{-1}(y - z \mod 26),$$

   where $z \in \mathbb{Z}_{26}$.

   Suppose that π is the following permutation of $\mathbb{Z}_{26}$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\pi(x)$	23	13	24	0	7	15	14	6	25	16	22	1	19

x	13	14	15	16	17	18	19	20	21	22	23	24	25
$\pi(x)$	18	5	11	17	2	21	12	20	4	10	9	3	8

   The following ciphertext has been encrypted using this stream cipher; use exhaustive key search to decrypt it:

   WRTCNRLDSAFARWKXFTXCZRNHNYPDTZUUKMPLUSOXNEUDO
   KLXRMCBKGRCCURR

3. (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 $1, \cdots, n$ 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 $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, \cdots, n\}$. 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.

4. (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.