Applied Cryptography: Homework 1

(Deadline: 10:00am, 2020/09/16)

Justify your answers with calculations, proofs, and programs.

1. (10 points, question 2.6, page 52 of the textbook) If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an **involutory key**. Find all the involutory keys in the *Shift Cipher* over $\mathbb{Z}_{26}$.

2. (20 points, question 2.11, page 52 of the textbook)

   (a) Suppose that $K = (a, b)$ is a key in an *Affine Cipher* over $\mathbb{Z}_n$. Prove that K is an involutory key if and only if $a^{-1} \bmod n = a$ and $b(a+1) \equiv 0 (\bmod\ n)$.

   (b) Determine all the involutory keys in the *Affine Cipher* over $\mathbb{Z}_{15}$.

3. (15 points, question 2.15, page 53 of the textbook) Determine the inverse of the following matrices over $\mathbb{Z}_{26}$:

   (a) $\begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}$

   (b) $\begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$

4. (15 points, question 2.16, page 53 of the textbook)

   (a) Suppose that π is the following permutation of $\{1, \ldots, 8\}$:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

   Compute the permutation π^{-1}.

   (b) Decrypt the following ciphertext, for a *Permutation Cipher* with $m = 8$, which was encrypted using the key π:

   `TGEEMNELNNTDROEOAAHDOETCSHAEIRLM.`