- **Problem 1**

  Let's clearify the message space $\mathscr{M}$, key space $\mathscr{K}$, and cipher space $\mathscr{C}$. For the Key space we have:

$$\mathscr{K} = \{0, 1, \cdots, 25\} = \mathbb{Z}_{26} \qquad\qquad |\mathscr{K}| = 26$$

  For the message and cipher text space, first we map each letter to a number as below:

$$0 \iff A \quad 1 \iff B \quad \cdots \quad 25 \iff Z$$

  Now we can conclude that the message ($\mathscr{M}$) and cipher ($\mathscr{C}$) space is the same and equal to:

$$\mathscr{M} = \mathscr{C} = \{\text{All Possible String of Letters A-Z}\}$$

- **Problem 2**

  (a)

$$\mathbf{Dec}_k(c_1, \cdots, c_n) = (m_1, \cdots, m_n) \qquad \text{With} \quad m_i = (c_i - b) \times a^{-1}$$

  Becase we need the inverse of a, it must be a unit so we could use its inverse.

  (b) BMVVK mapped to HELLO so we can conclude that:

$$\begin{array}{cccc} B \longleftrightarrow H & M \longleftrightarrow E & V \longleftrightarrow L & K \longleftrightarrow O \\ 1 \longleftrightarrow 7 & 12 \longleftrightarrow 4 & 21 \longleftrightarrow 11 & 10 \longleftrightarrow 14 \end{array}$$

$$\begin{array}{ll} c_1 \overset{26}{\equiv} am_1 + b & 1 \overset{26}{\equiv} 7\,(a) + b \\ c_2 \overset{26}{\equiv} am_2 + b & 12 \overset{26}{\equiv} 4\,(a) + b \\ c_3 \overset{26}{\equiv} am_3 + b & 11 \overset{26}{\equiv} 21(a) + b \\ c_5 \overset{26}{\equiv} am_5 + b & 10 \overset{26}{\equiv} 14(a) + b \end{array}$$

  By two first equations we get $-3(a) \overset{26}{\equiv} 12 - 1$ which implies that $3a \overset{26}{\equiv} -11$ which leads us to $3a \overset{26}{\equiv} 15$ and $a \overset{26}{\equiv} 5$, by putting this to each equations we get that $b \overset{26}{\equiv} 18$. Hence we get $(a, b) \overset{26}{\equiv} (5, 18)$

  (c) We have a decryption function with two unkown variables a and b which we need to recover to get the plain text. We use the letter frequency which means that the two most common letters in our text is F and E respectively and in the statistically perspective the two most common letters are A and T by mapping these two and knowing we need to recover two unkown variables we can solve for them.

$$\begin{array}{ll} \text{F} \longleftrightarrow \text{E} & \text{E} \longleftrightarrow \text{T} \\ (6) \longleftrightarrow (5) & (5) \longleftrightarrow (20) \end{array}$$

$$\begin{cases} 6 = 6a + b \\ 5 = 20a + b \end{cases}$$

  This gives us $-15a \overset{26}{\equiv} 1$ which means $11a \overset{26}{\equiv} 1$ which means a is the inverse of 11 modular 26 which is 19, so $a \overset{26}{\equiv} 19$ which means $b \overset{26}{\equiv} 15$. By this we get the plaintext as follows:
  " NEVERTRUSTAPEOPLEWITHTWOSECRETS ".

- **Problem 3**

  (i) Only using 26 letters:
  function of encryption is $am + b$ with a and b as variables. By the condition that a should be coprime with respect to 26 which makes possible values for a to be $\varphi(26) = \varphi(13)\varphi(2) = (12)(1) = 12$ we have 12 possibilities for a and 26 possibilities for b which gives us together $26 \times 12 = 312$ possibilities.

  (ii) letters plus (?) (.) (,) (!):
  In this case we are working with number $30 = 26 + 4$ with the same formula as previous part we have $\varphi(30) = \varphi(3)\varphi(2)\varphi(5) = 2 \times 1 \times 4 = 8$ possibilities for a and 30 possibilities for b which gives us together $8 \times 30 = 240$ possibilities.

- **Problem 4**
  Just use quipquip or any other substitution cipher solver, we get the text below:
  MATHEMATICSISTHEQUEENOFTHESCIENCESANDNUMBERTHEORYISTHEQUEENOFMATHEMATICSCARLFRIEDRICHGAUSS
  which is the phrase: Mathematics is the queen of the sciences and number theory is the queen of mathematics.
  By CARLFRIEDRICH GAUSS

- **Problem 5**
- **Problem 6**
- **Problem 7**
- **Problem 8**
- **Problem 9**
- **Problem 10**
- **Problem 11**