1. The key letter is 's' and the key word is 'impulse'. The name of the book is 'The Annotated Anne of Green Gables'. I found the relative frequency of each english letter in literature, say it's $a_1, a_2, \dots a_{26}$. Let $b_1, b_2, \dots b_{26}$ be the relative frequency in the ciphertext corresponding to the english alphabet. Find the permutations of b's that have larger value of $L = a_1c_1, a_2c_2, \dots a_{26}c_{26}$ where c_i's is a permutation of b_i's. Decode the ciphertext by the 5 permutations that have the largest value of L and see which one looks more like english.

2. (a) Solve the linear equation $c = mA + b$. Since A is invertable, $m = (c - b)A^{-1}$

   (b) Let $\boldsymbol{m} = \mathbf{0}$, then $\boldsymbol{c} = \boldsymbol{b}$. Then let $\boldsymbol{m_i}$ be the plaintext with the ith entry 1 and the rest all 0's. Get the corresponding ciphertext $\boldsymbol{c_i}$ and $\boldsymbol{c_i} - \boldsymbol{b}$ is the ith row of $\boldsymbol{A}$

   (c) Select any 3 ciphertext c_1, c_2, c_3 where $c_i \neq c, c_1 + c_2 - c_3 = c$. (there are many choices to do this and it's easy) Obtain the corresponding plaintexts m_1, m_2, m_3 and we have

$$\begin{aligned} m_1 A + b &= c_1 && (1) \\ m_2 A + b &= c_2 && (2) \\ m_3 A + b &= c_3 && (3) \\ (1) + (2) - (3) &\text{ we have} && (4) \\ (m_1 + m_2 - m_3)A + b &= (c_1 + c_2 - c_3) && (5) \\ & && (6) \end{aligned}$$

   Since the encryption is a one-to-one map, $m_1 + m_2 - m_3$ is the correspoinding plaintext for c.

3. (a) (Omiting the modulo notation) Denote the original permutation S_i^0 . For the first byte, $i = 1$, $j = 2$, $S[2] = S^0[1] = 2, S[1] = S^0[2]$, $t = S^0[2] + S^0[1]$. For the second byte, $i = 2$, $j = S[2] + 2 = 4$, $S[2] = S[4], S[4] = S[2]$ so $t = S[2] + S[4] = S^0[4] + S^0[1]$. Since S_i^0's is a permutation from 0 to 255, $S^0[2] \neq S^0[4]$, the first byte and the second are definitely different.

   (b) In the keystream Generator, i and j remain the same and thus the keystream has a repeating period at least 256 bytes as $i + 256 \equiv i \pmod{256}$. XOR the first 256-byte palaintext and cipertext gives the 256 byte keystream. The entire keystream is repeating pattern of these 256-byte keystream. We can XOR the ciphertext and the entire keystream to recover the whole plaintext.