CS 171 HW1

Q1. $\mathcal{M}$ = {strings over Englih Alphabet}

$\mathcal{K} = \{\mathcal{K}_1, \mathcal{K}_2\}$ where $\mathcal{K}_1$ = {all bijections from {a⋯z} to {a⋯z}} and $\mathcal{K}_2$ = {English Alphabet}

Gen: Choose a random $K = (\pi_1, \pi_2) \in \mathcal{K}$ where $\pi_1 \in \mathcal{K}_1$ & $\pi_2 \in \mathcal{K}_2$

$Enc_K(m_1 \cdots m_t)$: output $C_1 \cdots C_t$ where $C_i := [(\pi_1(m_i) + \pi_2) \bmod 26]$

$Dec_K(C_1 \cdots C_t)$: output $m_1 \cdots m_t$ where $m_i = [\pi_1^{-1}(((C_i - \pi_2) \bmod 26)]$

Correctnell: For each i, $\pi_1^{-1}(((\pi_1(m_i) + \pi_2) \bmod 26 - \pi_2) \bmod 26) = m_i$

Because both the substitution & shift cipher doesn't alter the frequency of original message's each letter, we can use one single frequency analysis attack on the final ciphertext to break it.

Q2. (i) Scan for repeating sequences in ciphertext which could represent the same message part being encrypted by the same segments of the key. The GCD of the distances between these sequences might be the product of t_1 & t_2 because this double Vigenere cipher is basically the same as one single vigenere cipher with single key t_3 with length $t_1 * t_2$.

(ii) With possible values of $t_1 \times t_2$, try each trial key length T, by segmenting the ciphertext into $C_1, C_{1+T}, C_{1+2T} \cdots$, then calculate the frequency T_i for each letter i in stream, Compute, for each T, $S_T = \sum_i T_i^2$ and find T that has S_T closest to 0.065

(iii) With this key length, we can use IOC to break this scheme as if it is a single Vigenere cipher.

Q3. For Shift cipher: plaintext of length 1 is enough because $C - m \bmod 26$ is the key.

Substitution cipher: Plaintext of length 25 is enough because we need to find all bijections the key (25 because the rest can be derived from the 25 bijections)

Vigenere ciphers: t Known: length t is enough because $C_i - m_i \bmod 26$ is K_i for $0 \leq i \leq t$

t unknown but t_{max} given: length t_{max} needed because t is only apparent when repeating patte appear