Problem 1. The plaintext hidden in the following ciphertext is part of a famous English play:

KPJDLCGS PVHQKWRK KCKRBKPJ DLCWILKR BGSKORKO VCVCNVEW OVQDLCIL YFIRRIGB IVSXQKRB DLCSVCXX PKRAOWYX HMXIKKRG XLGCXGWI NVEWCQYX CNKVRC

(a) Determine the index of coincidence $I_C$. What can you derive from it? 

Problem 2. The handling of long keys for Vernam ciphers is difficult. Therefore, autokey systems are proposed. For a given keyword $k = (k_0, \ldots, k_{n-1})$ and message $m = (m_0, \ldots, m_{l-1})$ the following two autokey systems are given.

$$c_i = \begin{cases} m_i + k_i \pmod{26} & 0 \leq i \leq n - 1 \\ m_i + c_{i-n} \pmod{26} & n \leq i \leq l - 1 \end{cases}$$

$$\hat{c}_i = \begin{cases} m_i + k_i \pmod{26} & 0 \leq i \leq n - 1 \\ m_i + m_{i-n} \pmod{26} & n \leq i \leq l - 1 \end{cases}$$

a) Describe a ciphertext-only attack on $c = (c_0, \ldots, c_{l-1})$.

b) Decrypt the cryptogram $c = DLGVTYOACOUVCEZA$.

c) Assume the keylength to be known. Describe a ciphertext-only attack on $\hat{c} = (\hat{c}_0, \ldots, \hat{c}_{l-1})$.

d) Decrypt the cryptogram $\hat{c} = QEXYIRVESIUXXKQVFLHKG$ using keylength 2.

Problem 3. (variance of the index of coincidence) In Lemma 3.3 of the lecture notes, the expectation value of the index of coincidence was calculated for the ciphertext $(C_1, \ldots, C_n)$ with random variables $C_1, \ldots, C_n$ i.i.d.

a) Derive the variance of the index of coincidence $\text{Var}(I_C)$ for the model of Lemma 3.3.

\[I_C \approx 0.0385: \text{polyalphabetic and uniformly distributed}; \ I_C \approx 0.0668: \text{monoalphabetic and English}\]