1. Your first mission is to perform a known-plaintext attack on each of the following types of cipher. In each case, you are given a ciphertext $C$ and the corresponding plaintext $M$. Your job is to find the key $K$. Tell exactly what you would do and how much of the key you would be able to discover. In each case, the alphabet is the usual 26 letters of English.
   a. A Caesar cipher (rotate the alphabet). The key is one letter of the alphabet.
   b. A simple substitution cipher, like the Cryptoquip in the *Exponent*. The key is a permutation of the alphabet.
   c. A Vigenère cipher with unknown key length. The key is a string of letters of unknown length $t$.

2. Suppose a Kasiski analysis identifies these six pairs of repeated sequences in the ciphertext of a Vigenère cipher:
   
   Location of start of first occurrence: 10 21 37 49 58 72
   Location of start of second occurrence: 34 63 109 103 162 132

   What can you conclude about the length $t$ of the key word used to encrypt the message? Explain your answer.

3. Consider the encryption scheme $\Pi$ similar to Vigenère's except that the key is a string of random letters as long as the plaintext. For $\Pi$ we have $M = K = C$. For enciphering messages $\ell$ letters long, $\text{Gen}$ chooses a random string of $\ell$ letters with uniform distribution, so that each such string $K = k_0k_1\ldots k_{\ell-1}$ has probability $26^{-\ell}$ of being chosen. $\text{Enc}$ and $\text{Dec}$ are given by the formulas $c_i = (m_i + k_i) \mod 26$ and $m_i = (c_i - k_i) \mod 26$.

   Prove or disprove: The scheme $\Pi$ is perfectly secret. Hint: Use Shannon's theorem.