1. Consider the ciphertext which was created using the Columnar encryption algorithm, as in Assignment 1: `e__culewT_mcety_eerno_oon.reyibnnshaahs__ar`

   It contains $n = 43$ characters. The symbol `_` denotes a space. The key is `[5, 1, 3, 4, 2]`,

   (a) Fill in a grid using the "shaded boxes" method from the textbook. Make sure to shade the appropriate boxes.

   (b) Given a message of length n, and the key of length k, what is the formula for the number of shaded boxes? Apply your formula to this example to verify that you have the right number of shaded boxes in the grid above.

   (c) Decrypt the message.

2. Alice and Bob use the quantum key exchange protocol:
   `+` for *rectilinear* , and `x` for *diagonal* filters;
   `-` for *horizontal* , and `|` for *vertical* vibration polarization;
   `\` for *backward diagonal*, and `/` for *forward diagonal* polarization.

   Alice uses `x+x+x ++x+x xx++x` for filter selection, and 00010 10100 11001 for key construction.
   Bob uses `+xx+x x++++ xxx++` for filter selection.

   (a) What polarization sequence does Alice send Bob? Show your work!

   (b) Show a possible sequence of Bob's photon measurments. How does Bob know which of his photon measurments are correct?

   (c) What is their final key? Show how you arrived at it.

   (d) How can Alice and Bob check for Eve's eavesdropping?

   (e) Consider the following statement: *When scientists manage to construct fully operational quantum computers, the system of encryption based on quantum cryptography will no longer be secure.* Explain why or why not.

3. Here is the start of a text in English encrypted using the Vigenere ciphertext:

   `W U E Q B V H Y F H N T X E E R S T K R S W E UF G U U R I`

   Statistics of the entire ciphertext (which is not shown):

```
Keylength 3 frequencies:
 A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
 0  3  1  8  1  5  5 23  0  0  8 11  1  0  1  1 14 10  0  0 11  5 12  1  0  2 123
 9 11  6  0 10  9 13  1  0  0  0  0  0  9  5  3  5 17  2  5  7  6  0  0  3  1 122
 9  5  2  5 14  6  3 11 15  0  0  4  4  5  5  3  0  5  5  8  6  1  2  1  3  0 122
Keylength 4 frequencies:
 A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
 5  5  3  7  5  6  5 10  2  0  2  2  2  3  2  3  7  4  2  5  5  1  4  1  1  0  92
 4  4  1  3  8  5  2 11  4  0  4  7  0  4  3  2  2  9  1  3  5  4  2  1  3  0  92
 5  6  2  0  8  5  6  7  3  0  2  4  1  5  3  0  4 10  1  2  6  4  6  0  0  2  92
 4  4  3  3  4  4  8  7  6  0  0  2  2  2  3  2  6  9  3  3  8  3  2  0  2  1  91
```

   Repeated trigram sequences with offsets: `RAE 108, BGH 91, GHH 39, IQT 24, IQR 66, ...`

   (a) Compute the IC value of the 30-letter ciphertext above. Show your work.

   (b) What is the most likely keyword length? Explain your reasoning.

   (c) Which repeated trigrams are likely occurring by accident? Explain.

   (d) What is the keyword? Explain how you found it. (*Hint: it's a well-known acronym.*)

   (e) Decrypt the first 20 characters of the ciphertext into English.

4. Alice and Bob come up with a novel idea for a DHM-like message exchange scheme based on the double-padlock principle. It does not require Alice and Bob to share a secret key.

   Here is how it works:

   - Alice and Bob select their own keys a and b, and keep them secret.
   - Alice encrypts her message m with her secret key a, and sends the ciphertext C1 to Bob.
   - After receiving C1, Bob encrypts it again with his secret key b, and sends the resulting ciphertext C2 to Alice.
   - After receiving C2, Alice decrypts it with her secret key a, and sends the resulting ciphertext C3 back to Bob.
   - Finally, Bob receives C3 and decrypts it with his secret key b to get Alice's message m.

   (a) What type of cipher must be used for the above scheme to work correctly? Would it work if a substitution cipher was used for encryption? Explain.

   (b) Play the role of Eve who, intercepts the three ciphertexts below. Eve guesses that Alice and Bob are using the Vigenere cipher with 3-letter dictionary words as their keys. Crack the following exchange. Show your work.

   `C1 = VWDDSD`   `C2 = WAWEWW`   `C3 = LMLTIL`

   (c) Eve intercepts Alice's C1 and C3, but fails to intercept Bob's C2. Explain how Eve could still crack Alice's message m if Alice and Bob use the Vigenere cipher.

   (d) Alice and Bob become more cautious and start using completely random keys that are as long as the messages. Can Eve still crack Alice's messages? Explain how it can be done, or why it can't.

5. Recall that in Assignment 8, you implemented a method to crack a poorly-designed public-key system.

   (a) Create your public key using $p = 3$ and $q = 5$ as your primes. What is your public key?

   (b) Create your private key to accompany your public key in (a). What is your private key?

   (c) Encode the message "BACK" using your public key in (a) and a block size of 1, as in Assignment 8. Assume that the value of M is the index of the character in the symbol set `ABCDEFGHIJKLMNOPQRSTUVQXYZ`. What is the ciphertext?

   (d) Decode the following ciphertext: [12].

   (e) Provide at least two reasons why the public-key system that you have created in this should not be used for secret communication.

6. Recall that in Assignment 9, you implemented a function `keyScore` which computes the n-gram score (a floating-point number) of a decipherment attempt.

   For this question, write Python code for the `ngramScore` function below which returns the n-gram score of a decipherment string. The function take three parameters:

   - `decipherment` is a string that contains the attempted decipherment.
   - `englishText` is a string that contains the text used for computing the frequencies of n-grams. (It contains only uppercase letters and spaces.)
   - n is the n-gram size.

   For example, the following function call should return the value of approximately 0.375.
   `ngramScore( 'MX COOK BOOK', 'THE PHONE BOOTH HAD A COOPER HOOK', 2 )`

7. Archeologists unearthed ancient tablets written in a syllabic CV-type script similar to Linear B. Use the method of Alice Kober to perform the decipherment.

   The words found on the tablets include the following:

   $\perp\triangle\sqcap$ $\qquad$ $\bowtie\uplus\exists\mp$ $\qquad$ $\bowtie\uplus\in$ $\qquad$ $\perp\triangle\mp$ $\qquad$ $\perp\bowtie$ $\qquad$ $\bowtie\uplus\exists\sqcap$

   (a) Organize the words that share inflectional patterns into two tables.

   (b) Which symbols represent the bridging syllables?

   (c) Organize four of the symbols into a 2x2 grid. Explain your choices.

   (d) Suppose that the following words have been correctly deciphered:

   $\bowtie\exists =$ doye $\qquad$ $\uplus\mp =$ bite $\qquad$ $\odot\uplus\sqcap =$ lubimu

   Reconstruct the case endings for all three cases.