Shift Cipher Decrypter

Shift cipher is a simple encryption method. When encrypting a message, every letter in the original message is replaced by a different letter *k* positions down the alphabet (modulo by 26), where *k* is an integer.

In the following example for $k = 8$,

Original message: `WORK HARD, PLAY HARD!`

↓ Shifting *k* positions down the alphabet (modulo by 26)

Cipher text: `EWZS PIZL, XTIG PIZL!`

Note:

1. Assume that the message only contains upper case letters, space characters and punctuation marks.
2. Space characters and punctuation marks remain unchanged during the encryption.

A shift cipher decrypter can guess the message without knowing *k*. If a message is long enough, the mo frequent letter will be 'E'.

Task 1 (Design & Implementation)

Write a program to implement the shift cipher decrypter. You are advised to run your program with a messa of at least 200 words such that the alphabet distribution follows the general pattern. Do the following task

(a) Select suitable data types.
(b) Count the letter frequencies of the cipher text.
(c) Find the possible values of *k* .
(d) By using stepwise refinement, describe the algorithms for decryption.
(e) Use a flowchart to describe the algorithms in (d).

You may want to consider some of the following key factors when designing the program:

- data structure
- variable declaration and initialization
- data collection, input and validation
- data processing
- program output
- interface of the program
- modularity
- reusability
- portability
- system development cycle
- sorting and searching algorithm

Create a presentation and/or documents to briefly describe the components involved in designing the program.