EE212-Microprocessors Off-Lab Assignment 2 Section 2

Spring 2022

1 Introduction

Practise of secure communication is a must for protecting the parties against adversarial actions. Therefore, there are numerous method to cipher the messages and deliver them safely [1]. In this assignment, you will implement a simple method to decipher an encoded message. You are required to decipher a text encoded with pivot cipher. In this cipher, pivot letter can be considered as the origin of a mirrored alphabet.

2 Implementation

In this assignment, your task is to decrypt a null-terminated single-word all-capital-letters text saved in the internal memory (ROM) of 8051 (consisting of characters only from the English alphabet capital letters) and show the deciphered text on the LCD display. You will be using two software programs: (i) MCU 8051 IDE, for simulation of your code and (ii) Proteus, for setting up the required hardware setup and demonstrating your work with an LCD. You can assume that the word you will be reading is all in `ASCII` format and implement the decryption program accordingly (For checking the correctness of your code, you can write a test word to the ROM either using the DB directive like the following `MYWORD: DB "TEST"` or still use the same `DB` directive but check [2] to write the individual `ASCII` characters one by one.)

You are provided the position of a known character in the encoded ROM data. Since you know the position of this character and its decoded value is provided to you, you can implement a code to try the possible pivots or find it by averaging the letter positions. For example, if you have the following encoded text **LAMLU** in the ROM, the known character is **K** and its index in the text is **4** (assume a 0-based array indexing, i.e., indices are starting with 0), then, you should match the character at index 4 in the encoded text with **K**. You can see that **K** is 10 letters away from **U**. Now, consider the alphabets given below.

- **U**VWXYZAB**C**DEFGHIJ**K**LMNOPQRST and,
- **K**LMNO**P**QRST**U**VWXYZABCDEFGHIJ

Note that, **C** and **P** can be a pivot because, those two letters are equally distanced to **K** and **U**. Actually, it doesn't matter if you choose the pivot as **P** or **C** because of the symmetry. If you try the next characters in the encoded text, you can find that the decoded message is **TESTK**. Since **K** is given as a hint, you can omit it. To find the pivot, you can try to take the average of position of **K**(10) and **U**(20). Thus, the pivot position can be found as **P**(15). You can check the python script for testing and generating examples.

Now after finding the key, think about how the encryption algorithm can be implemented.

3 Assumptions

- There are three information you can use; encoded text, the known character and its index in the encoded text.
- A positive shift after the letter 'Z' rolls over and continues with 'A'. Similarly, a negative shift that goes backward after the letter 'A' continues with 'Z', 'Y', ... etc.
- Text is short enough to fit the LCD.

References

[1] Contributors to Wikimedia projects. *Cryptography - Wikipedia*. [Online; accessed 26. Feb. 2022]. Nov. 2001. URL: `https://en.wikipedia.org/w/index.php?title=Cryptography&oldid=1074103510`.

[2] *Hex to ASCII | Hex to Text converter*. [Online; accessed 26. Feb. 2022]. Jan. 2022. URL: `https://www.rapidtables.com/convert/number/hex-to-ascii.html`.