EE212-Microprocessors Off-Lab Assignment 2 Section 1

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 [2]. In this assignment, you will implement a simple method to decipher an encoded message. You are required to decipher a text encoded with modified Caesar cipher [1]. The modification is, the shift value increases with each letter in the message (progressive-shift) [4].

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 [3] 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 shifts in modified Caesar cipher and find the correct shift value (key). If your trial of a shifted value matches with the encoded character in the ROM, you will use this shift value to decode the rest of the encoded text. For example, if you have the following encoded text **YKRAC** in the ROM, the known character is **K** and its index in the text is **2** (assume a 0-based array indexing, i.e., indices are starting with 0), then, you should match the character at index 2 in the encoded text with **K**. In the text, the character is **R**. Hence, the shift is 7. This means that this cipher maps all the letters in the encoded text to the letter in the alphabet five characters away from the original letter. To find this key/shift, you can iterate over the values starting from 0 to 26 in a brute-force search or just find the difference between the two letters. Note that, the shift value 7 is applied on the index 2. Thus, the shifts start from 5 and increases with every letter. 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. *Caesar cipher - Wikipedia.* [Online; accessed 26. Feb. 2022]. Jan. 2022. URL: `https://en.wikipedia.org/w/index.php?title=Caesar_cipher&oldid=1068571131`.

[2] 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`.

[3] *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`.

[4] *Progressive Caesar Cipher - Online Decoder, Encoder, Translator.* [Online; accessed 27. Feb. 2022]. Feb. 2022. URL: `https://www.dcode.fr/progressive-caesar-cipher`.