DESIGN OF DIGITAL SYSTEMS (CO202)
MINI PROJECT (2017-18)

ABSTRACT

ENCRYPTION AND DECRYPTION USING CAESER SHIFT CIPHER

Guided by:
Dr. B. R. Chandavarkar

Submitted by:
Namrata Ladda (16CO121)
Aditi Gupta (16CO202)

- ## Overview:

  The Caeser Shift Cipher is a monoalphabetic substitution cipher wherein each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. To cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

- ## Encryption/Decryption:

  The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as

  $E_n(x) = (x+n) \bmod 26$ [Encryption Phase with shift n]
  $D_n(x) = (x-n) \bmod 26$ [Decryption Phase with shift n]

- ## Algorithm:

  Input and Output: A string of lower case letters, called Text is taken as input using 26 buttons available for each alphabet. An integer between 0-25 denoting the required shift is also inputted. The output is obtained in form of respective LED being lit up corresponding to the input character (encryption and decryption are done one character at a time).

  Procedure: Traverse the given text one character at a time. For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text. Return the new string generated. An example is shown below:

  Text : ATTACKATONCE
  Shift: 4

Cipher: EXXEGOEXSRGI

- Components required:

1. Multiplexers
2. Basic logic gates
3. Shift registers
4. Counter
5. Decoder/ Encoder
6. LEDs

- References:

1. http://crypto.interactive-maths.com/caesar-shift-cipher.html
2. *https://learncryptography.com/classical-encryption/caesar-cipher*
3. *http://www.geeksforgeeks.org/caesar-cipher/*