Design And Implementation of A Miniature Encryption System Using Variable 4-Bit Cipher Key and Ps2 Keyboard Interface In A Spartan 3e Fpga Kit

S. Arvindh, Soham Majumder, Bodhisatta pramanik, Gourab halder, Soham samanta
Department of Electronics and Communication Engineering
Netaji Subhash Engineering College, Kolkata, West Bengal, India

Paramita Choudhury
Associate professor
Department of Electronics and Communication Engineering
Netaji Subhash Engineering College, Kolkata, West Bengal, India

Abstract- An encryption system is a security system, by which the confidentiality of data is maintained. It has varied uses in almost every sector, as the present world scenario requires efficient and secure exchange of information. It is highly desirable to make this transfer such that, no one other that the intended users can access the information. An encryption system solves this purpose. The objective of the project is to design an entry level encryption system, in which a particular data (only alphabets in this case) is encrypted using the CEASER cipher technique, using a 4-bit cipher text to be input by the user. The security system is the basic building block for further developments in encryption.

Keywords – FPGA, encryption, security, Verilog

I. INTRODUCTION

An encryption system is basically a security system, by which the confidentiality of data is maintained. It has varied uses in almost every sector, as the present world scenario requires efficient and secure exchange of information. It is highly desirable to make this transfer such that, no one other that the intended users can access the information. An encryption system solves this purpose.

The design technique is such that there are three major modules used in building the system. The initial block includes a finite state machine to interface a PS2 device(in this case a keyboard) , and accept the alphabet input from the keyboard.

The second block performs the encryption on the data inputted by the user. A 4 bit cipher is taken as input, and the encryption algorithm is put to use.

The third block involves another finite state machine which initiates the process of interfacing the 44780 Hitachi LCD controller in order to display the encrypted data in the LCD display. The data so encrypted can be sent over serial communication channels.

The rest of the paper is organized as follows. Proposed encryption algorithm is explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

II. PROPOSED ALGORITHM

A. Encryption algorithm –

The 8 bit ASCII CODE, generated in the PS2 module is fed into an encryption system, which forms the center of the system. The inputs to the module are the 8 BIT ASCII CODE and A 4 BIT USER PROVIDED CIPHER KEY. We have used the 4 slide switches provided in the FPGA KIT as our inputs of the 4 bit cipher. The ASCII code, along with the cipher key is bitwise subtracted in order to generate a 8 bit binary code, which is our encrypted data. As this is a miniature system, the encrypting procedure has been kept relatively simple. However, many other operations can be performed in this module. However, a major part of this encryption system is that it's designed in a cyclic

alphabetical order, such that the encrypted data is also an alphabet, which is –x times the original alphabet. The following diagram (shown in the next page) shows the encrypting procedure more vividly.

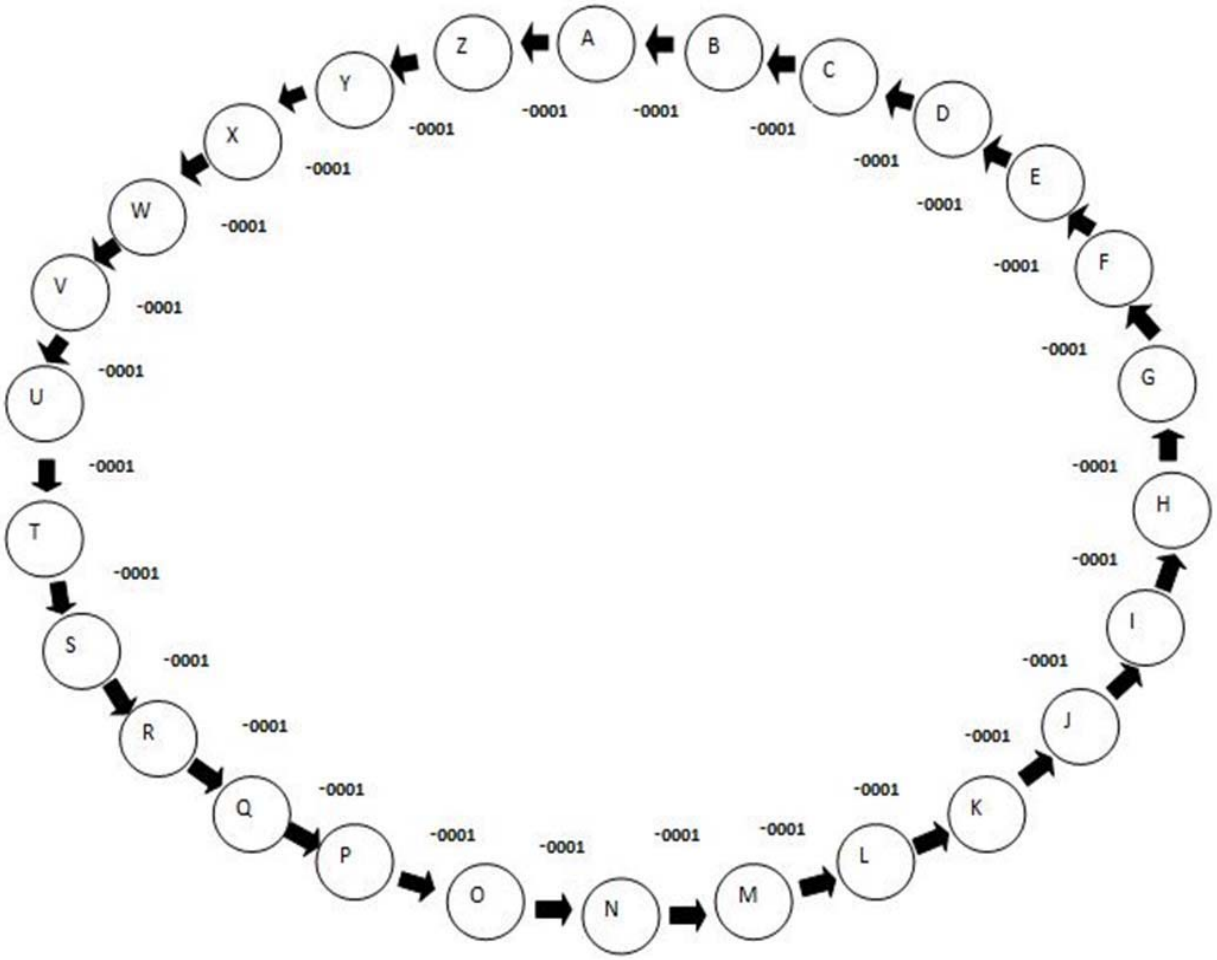


Figure 1. Ceaser cipher model

Suppose the input is A, and the cipher is 0011, then according to the figure, the encrypted alphabet will be

$$(A - 0011) = (((A - 0001) - 0001) - 0001);$$
$$= ((Z - 0001) - 0001);$$
$$= (Y - 0001);$$
$$= X$$

X is the encrypted value. This can easily be checked from the diagram given in the previous page.

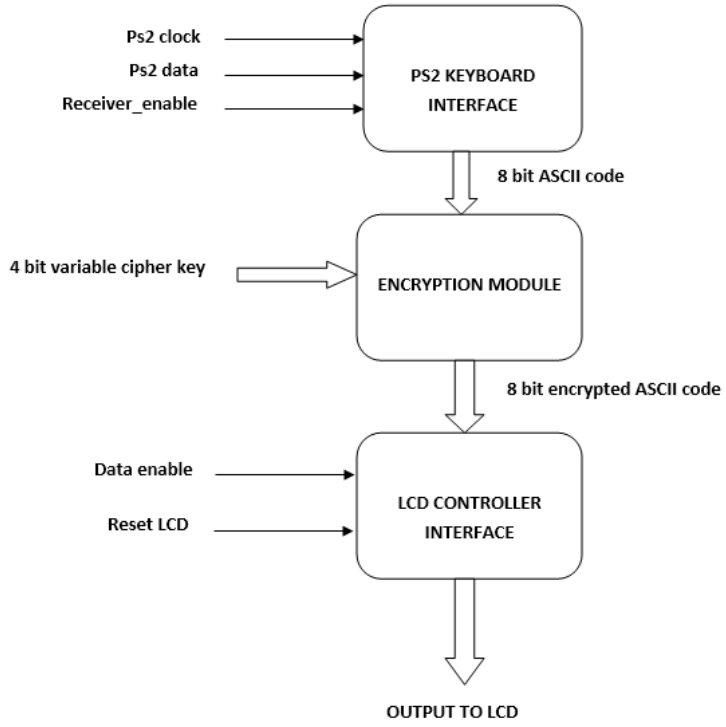


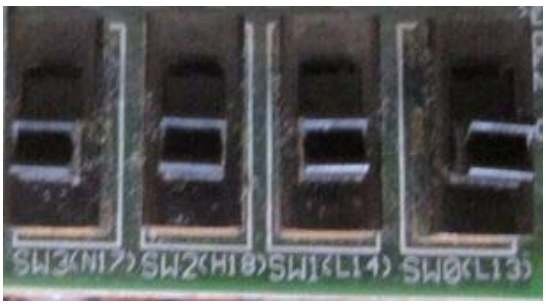
Figure 2: Encryption algorithm Block Diagram

III. EXPERIMENT AND RESULT

The kit used for the design and testing of the system is a XILINX XC3S500E FPGA starter kit. The ps2 port is used to connect the keyboard, the 4slide switches enable the user to input the cipher of his/her choice, the push buttons help to initiate the display, and to clear the LCD display.
Two cases are demonstrated as follows:
First, the cipher is kept "0" and the letter "G" is entered from the keyboard. Since the cipher is "0", the letter "G" will be displayed on the LCD.
For the next case, the LCD display is cleared with the help of the push buttons on the FPGA kit, and the cipher set to "0011" i.e. 3. The letter "G" is again typed in from the keyboard and the encrypted letter "D" is obtained on the LCD display. The procedures and results along with their diagrammatic illustrations have been provided.

Step1:

Cipher is being set to "0".

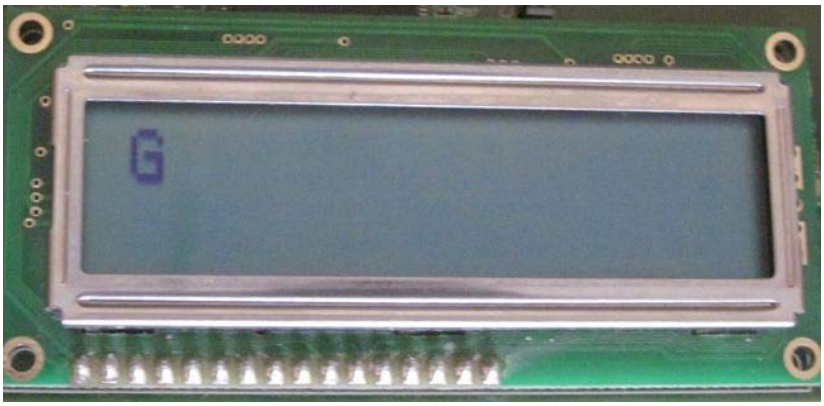


Step 2:

The letter “G” is entered from the keyboard.

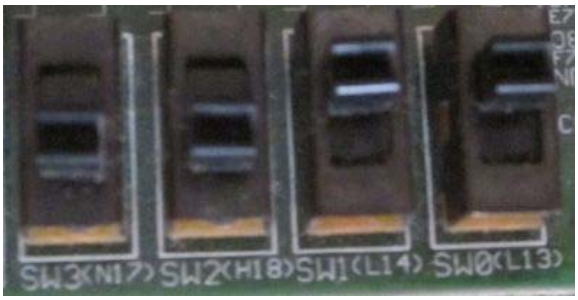
Result:

Since cipher is 0, the output obtained will be “G” only.



Step 3:

Now the cipher has been set to “0011” i.e “3”

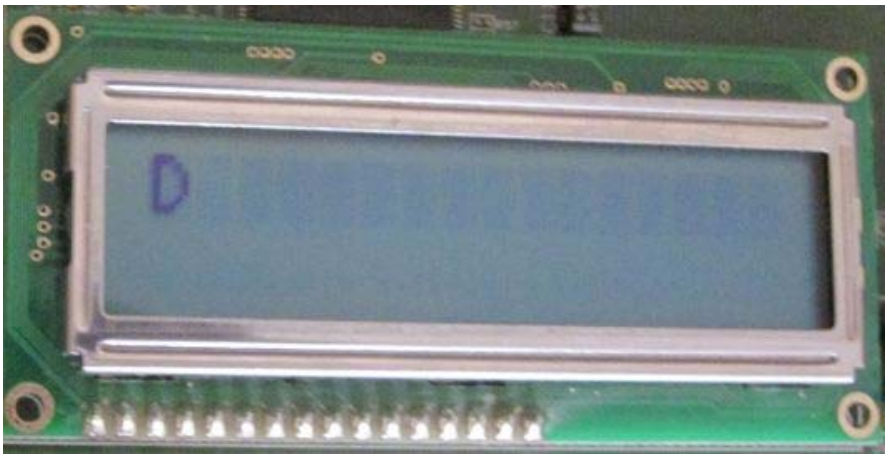


Step 4:

The letter “G” is entered from the keyboard.

Result:

Since the cipher is 3, an encrypted letter will be displayed at the output. For this case “D” will be displayed on the LCD.



Hence the encrypted letter is obtained at the output, based on the value of the cipher. At the end of the display, the LCD will be reset using the push buttons provided on the SPARTAN FPGA kit, and the next letter needed to be encrypted will be entered from the keyboard.

IV.CONCLUSION

This is an entry level encryption system, which can be further enhanced and modified to be used in a security system. A basic cryptographic system involves both the encryption system as well as the decryption system. The project is just one half of the entire system. A few control signals, a change in the LOOK UP TABLES will solve the purpose. The project also aims to show enthusiasts the very essence of an encryption system. They can develop a much complex system, integrating this system as one of the basic building blocks.

REFERENCES

[1] FPGA PROTOTYPING BY VERILOG EXAMPLES (Xilinx SpartanTM-3 Version) by Pong P. Chu (Cleveland State University)

[2] HD44780U (LCD-II) USER GUIDE, ADE-207-272(Z), '99.9, Rev. 0.0

[3] The PS/2 Mouse/Keyboard Protocol (Sou rce: http://www.Computer-Engineering.org) Author: Adam Chapweske