**COL215: Mini Project (Week 11)**

**Student_1: Pavas Goyal (2018CS10363)**

**Student_2: Dipen Kumar(2018CS50098)**

**Project 1- Text encryption/decryption ( Crypto – box)**

**AIM:**

To encrypt/decrypt data performing some logic operations. It allows you to securely protect data that you don't want anyone else to have access to.

**Specification:**

Serial receiver and transmitter provides the interface for memory module for downloading (PC to BASYS-3) and uploading files (BASYS-3 to PC). The downloaded data before being stored into memory will be encrypted/decrypted depending on the selected mode of input. The encryption will be done using a key (which can be user-specified/default) by simple stream cipher cryptography.

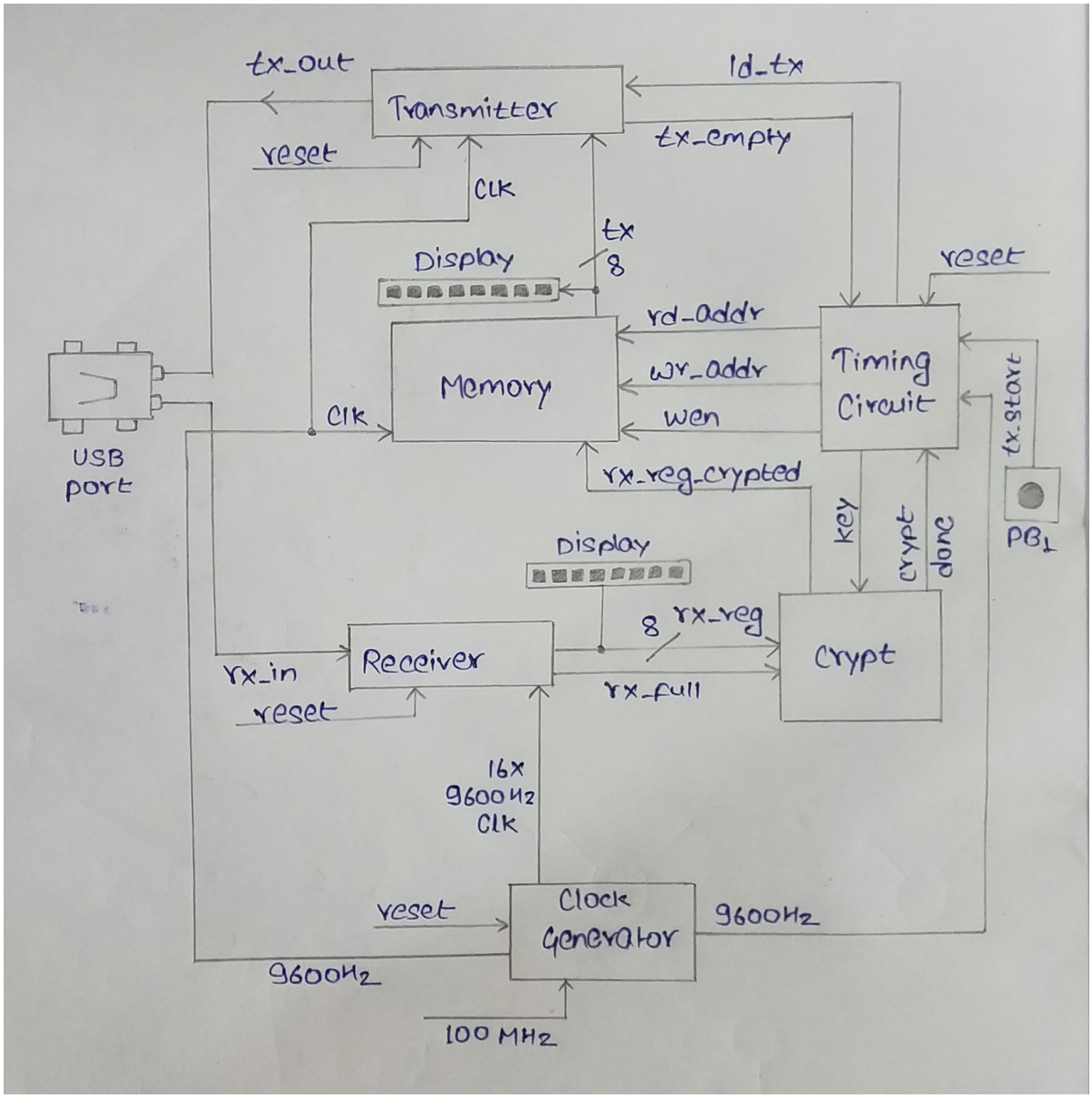
**Details:**

We are using 8 slide switches for user to enter the key used for encrypting/decrypting. That key xor the input data will give up encrypted/decrypted data. Encrypter/Decrypter module will take input from receiver module and perform bit by bit xor operation and pass to memory module. Timing module will signal transmitter module when encryption/decryption is done to transmit processed data.

Another slide switch will be used to select the mode of either encryption or decryption. At last one more will be used to select between two mode- one in which user will enter the value of key another in which a default inbuilt key will be used.

Two push button named transmit and reset which will signal the memory module to transmit and clear the memory respectively are also used.

A simple brief block diagram of our crypto-box is shown below.




**Design and brief description of various components/module:**

Timing- It generates memory address where data received by receiver is written and read. It also generate write enable signal. When tx_start signal the timing circuit, it starts generating read address and give to transmitter. It wait till transmitter transmit it and after transmitter is done its job it check for availability of another read address. If it is available it generate another and

pass to transmitter and so on continues till all read address has been passed. After that it again goes back to the state where it will again check for tx_start signal. If crypt signal is '0' that means it is encrypting/decrypting data then timing circuit will wait for it and when done it will produce write enable signal and write address. Memory will then do its job of writing the received data.

Memory- PB1 push button signal to transmit the data received and stored in memory to the parallel input of transmitter.

Crypt- It performs logic operation of the data received by receiver to transform it into some other not-recognizable form. It then pass this encrypted data to memory to store and further through memory to transmitter to transmit.

Receiver- It takes serial input of the data and give parallel output to crypt. It check for start bit 0 and then with frequency of 9600 Hz it starts reading 8 data bit. At last it also verify stop bit.

Transmitter- It takes parallel input from memory and transmit data serially. It start transmitting when PB1 signal it with a frequency of 9600 Hz.

**Real Application of Text encryption/decryption:**

Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications to protect data.

Businesses use it to protect corporate secrets, governments use it to secure classified information, and many individuals use it to protect personal information to guard against things like identity theft.

Espionage uses encryption to securely protect folder contents, which could contain emails, chat histories, tax information, credit card numbers, or any other sensitive information. This way, even if your computer is stolen that data is safe.