ED-Crypt

Ethernet Dongle for Encryption Decryption

10/2/2010

Akash Singh (2008CS10154)
Anshul Jain (2008CS10160)
Aseem Garg (2008CS10165)
Ujjaval Kumar Singh (2008CS10196)

INDEX

Motivation

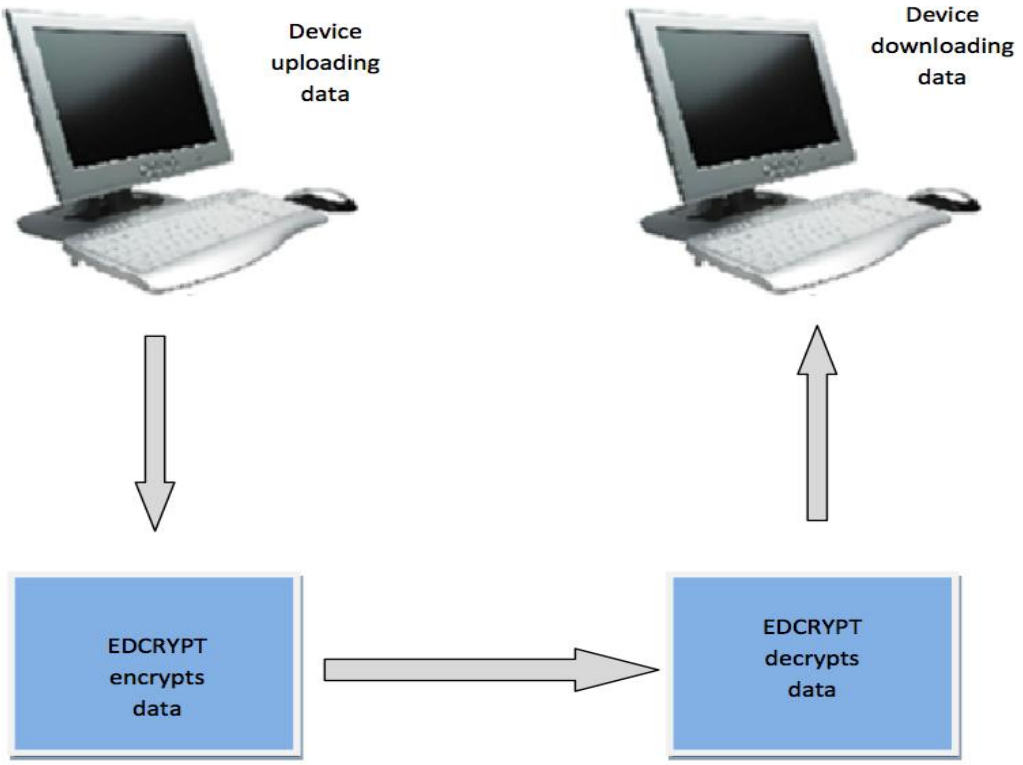
Encryption in real time: Encryption in software usually takes a long time due to the high computational work involved. Implementation of such algorithms in hardware would give the speeds required to encrypt/decrypt data on the fly.

Security: Even the most well written encryption programs are susceptible to attack from various kinds of viruses and trojans that forcibly insert a backdoor in the program running or manage to extract the key during the encryption process. Implementing such algorithms outside of main operating system makes the communication lot more secure.

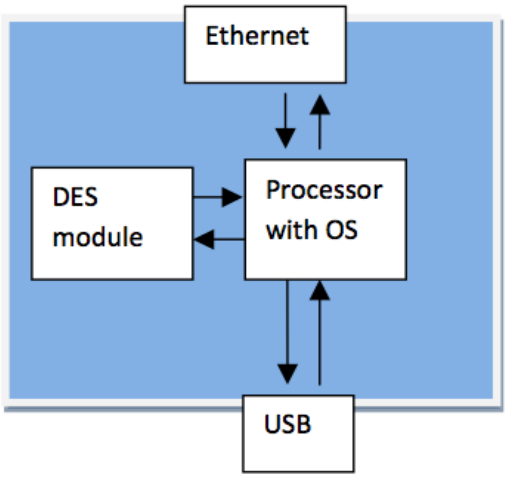
Objective

Objective is to implement an initial prototype of EDCrypt module to demonstrate the encryption of data that is input through the USB and relaying it to the ethernet that outputs it, and also decryption of data that is input through the ethernet and relaying it to the USB port that outputs it. This will be done while on the fly i.e. while the process for encryption/decryption is running, the data is being input and output simultaneously.

Design



ED-Crypt Module:

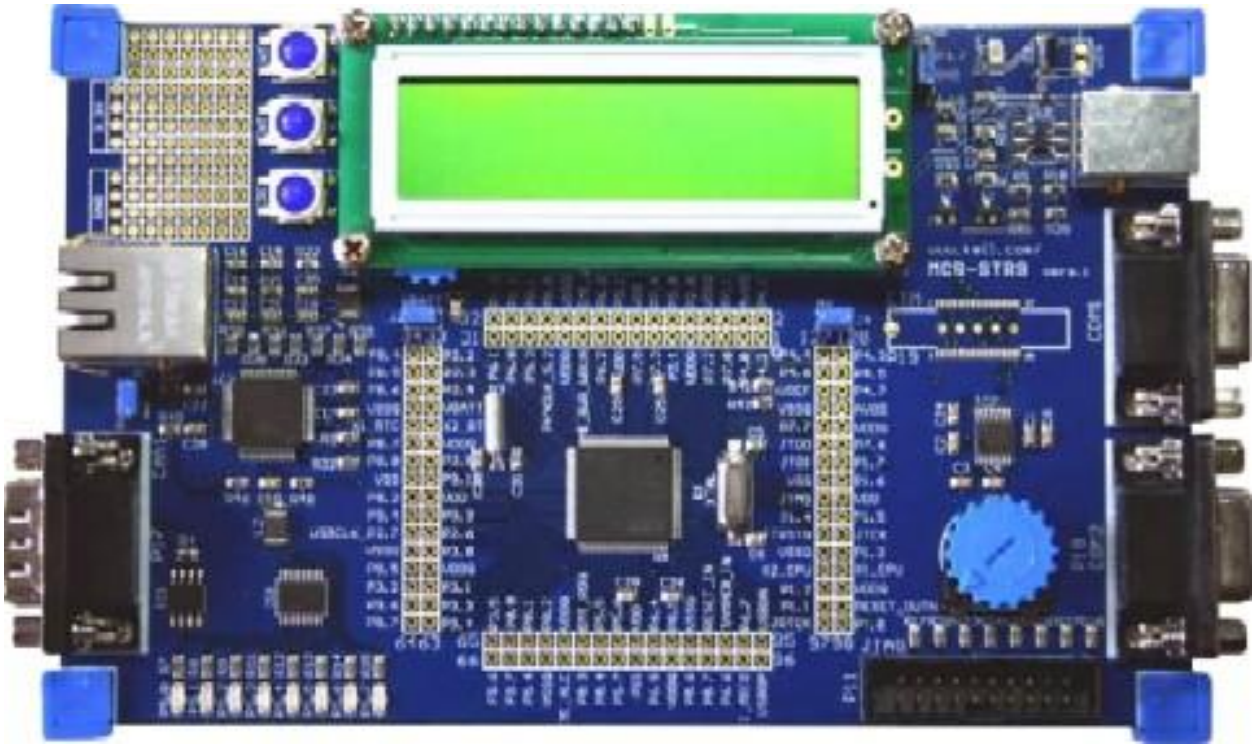


Hardware:

We have decided to work on MCBSTR9 board by Keil. It uses ARM 9 based str9 microcontroller developed by ST microelectronics. This board has ethernet as well as USB capabilities and hence will be used to implement USB and ethernet interfaces for our devices.

To implement encryption & decryption module we will use Virtex 2 Pro fpga board by Digilent. The module will be burnt on the FPGA chip.

These two boards will communicate using the GPIO pins on the Keil board and the Additional IO pins on the Digilent board, connected using wires.



MBSTR9

Software:

The Keil board will run the RTX OS (OS by Keil). RL-ARM library and its API's will be used for using the ethernet and USB port for data transfer. For implementing the above software on the board we use the uVision Microcontroller Development Kit.

On the V2Pro board we will use a hardware implementation of the DES algorithm for encryption/Decryption. To burn the above module on the board we will use the Xilinx ISE.

Status

- Learned to use GPIO pins on the microcontroller board and the Additional IO pins on the FPGA board.

- Developed some test programs and tested the speeds obtained on these ports using oscilloscope.

- Learned the use of RTX OS. Read about the scheduler and scheduled custom tasks on the OS.

- Learned the use of TCP/ UDP and developed some test programs.

- Working on USB: Started work on USB on both client and PC side.

- Started reading for DES module.

Plan & Time Line

Work Completed:

- Identifying and procuring the board, getting familiarity with programming on and using of the RTX OS (using MDK and uVision).

- Reading about the RL-ARM libraries. Gaining familiarity to work with Socket programming APIs provided.

- Started studying about USB programming on the PC side and the API for RL-ARM libraries for the USB on the MCBSTR9 board.

October:

- Week 1, 2, 3: Studying USB protocol and implementing the USB interface on the PC side and on the board.

- Week 3, 4: Studying the DES encryption algorithm in detail and Implementing it on the FPGA.

November:

- Week 1: Integrating the above mentioned DES module with the processor on the board.

- Week 2,3: Running tests on the device developed, optimization and fine tuning of all the modules.