DALHOUSIE UNIVERSITY
FACULTY OF ENGINEERING

CYBERCLAN™

Department of Electrical & Computer Engineering

Hardware Encryption Key

Team 2: Brad Jones
Dylan Mansfield
Patrick Oldfield
Zeynep Cetin

Project Definition

Develop a military-grade hardware key used for encryption. Proof of concept is expected to provide the fundamentals of hardware and software design for asymmetric encryption.

Relevance

- Hardware Encryption Key is motivated by the client's need for a higher level of security.
- Several software-based encryption products currently exist on the market, however none incorporate physical devices in their security schemes.
- Implementing encryption through hardware serves as an augment in security, providing an additional form of paranoia to infiltrators attempting to exploit media.

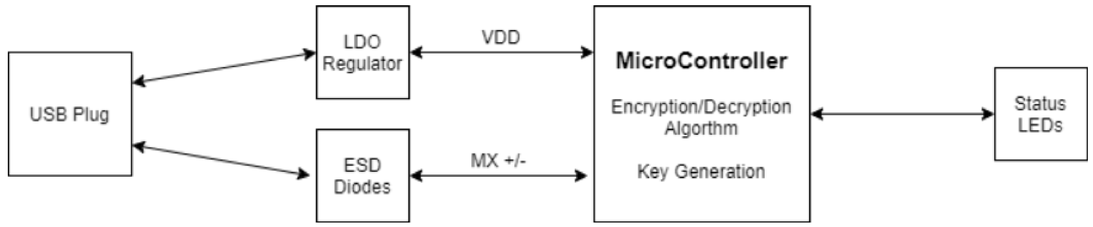
Deliverables

- Working script in IDE
- Performance diagnostics
- Establish HW requirements
- Select Microcontroller
- Preliminary schematics
- Prototype PCB design
  - Ideally as compact as possible

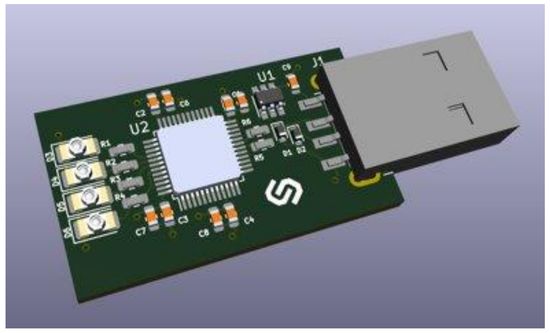
Microcontroller Selection

- STM32F401RE
- Breakout board for dev
- 512kB flash
- 96kB RAM
- MicroPython compatible
- AES Accelerator

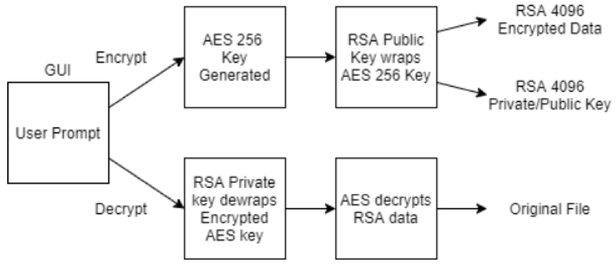
Details of Design



- USB type-A is implemented as the computer interface and was chosen for the simplistic pinout, in addition to meeting satisfactory data requirements.
- The USB serves as an interface connecting the host computer to the STM32F401RE microcontroller which is programmed with the encryption algorithm.

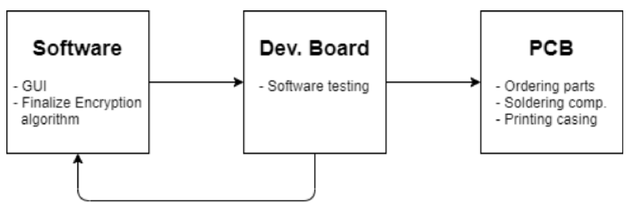


- An LDO has been included to step down 5V provided from the USB interface to 3V3. This is used to supply power to the microcontroller.
- ESD Diodes have been included for static electricity countermeasures, protecting the circuit from high-voltage electrostatic discharge entering from USB lines.
- Status LEDs have also been included to indicate when the device is powered, when the encryption algorithm is running, when the encryption algorithm has completed, and when the device is ready for a safe eject.
- A data flow diagram is shown to highlight the actions executed by the microcontroller



Future Work

- Part Ordering
- Code development for GUI and micro
- Finalizing code
- PCB milling/ordering
- Soldering components
- PCB testing



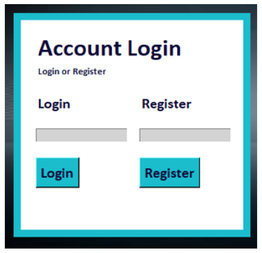
Encryption Algorithm

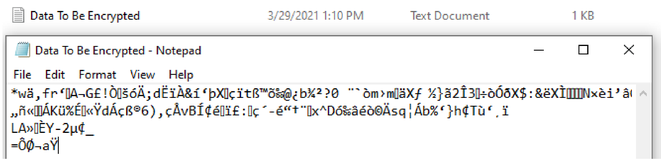
Primary components of the encryption algorithm:

- Registering: creating a key (RSA 4096 private/public key)
  - Password is used to wrap RSA 4096 private key with AES 256 key
- Encryption:
  - Create AES 256 key
  - Encrypt data using AES 256 key
  - Use RSA public key to encrypt AES key
- Decryption:
  - Requires password to access RSA 4096 private key
  - Uses private key to decrypt AES 256 key
  - AES 256 key decrypts data

Results

- Upon code execution, a GUI is opened and prompts the user to input their intentions.
- The GUI allows the user to encrypt, or decrypt files. All windows files may be encrypted.
- Example of .txt file upon encryption shown below





Acknowledgments

Team 2 would like to thank Bryan McNeil of CyberClan for his confidence in us to deploy Hardware encryption key, and for providing continual support and direction throughout the project.

The Team would like to extend thanks to Dr. Colin O'Flynn for providing insightful knowledge and supervision throughout the duration of this project.