DALHOUSIE UNIVERSITY
FACULTY OF ENGINEERING

CYBERCLAN™

Group 15
Daemon Watson – B00794990
Cameron Maher – B00763635
Matthew Paul – B00761317

Client: Richard D’Souza of CyberClan
Internal Supervisor: Dr. Larry Hughes

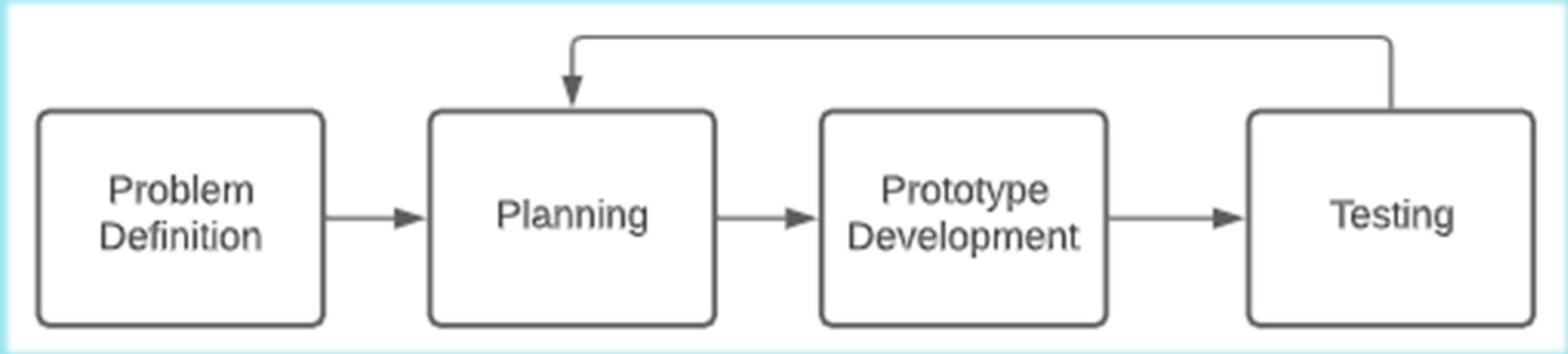
Department of Electrical Engineering

Hardware Encryption Key (HEK) – Phase 2

Background

- This project is sponsored by CyberClan who specializes in cyber security and provides incident response services.
- CyberClan has tasked us with creating a military-grade hardware encryption key (HEK) used for file encryption.
- The HEK is intended to be used by entities that require encryption for classified/protected data.
- Only select individuals can decrypt the encrypted files and recover the original file contents.

Design Process



Problem Definition:

- Met with Richard D’Souza of CyberClan to identify desired features and problems to be solved.

Planning:

- System software will be developed, followed by the design of the system hardware.

Prototype Development:

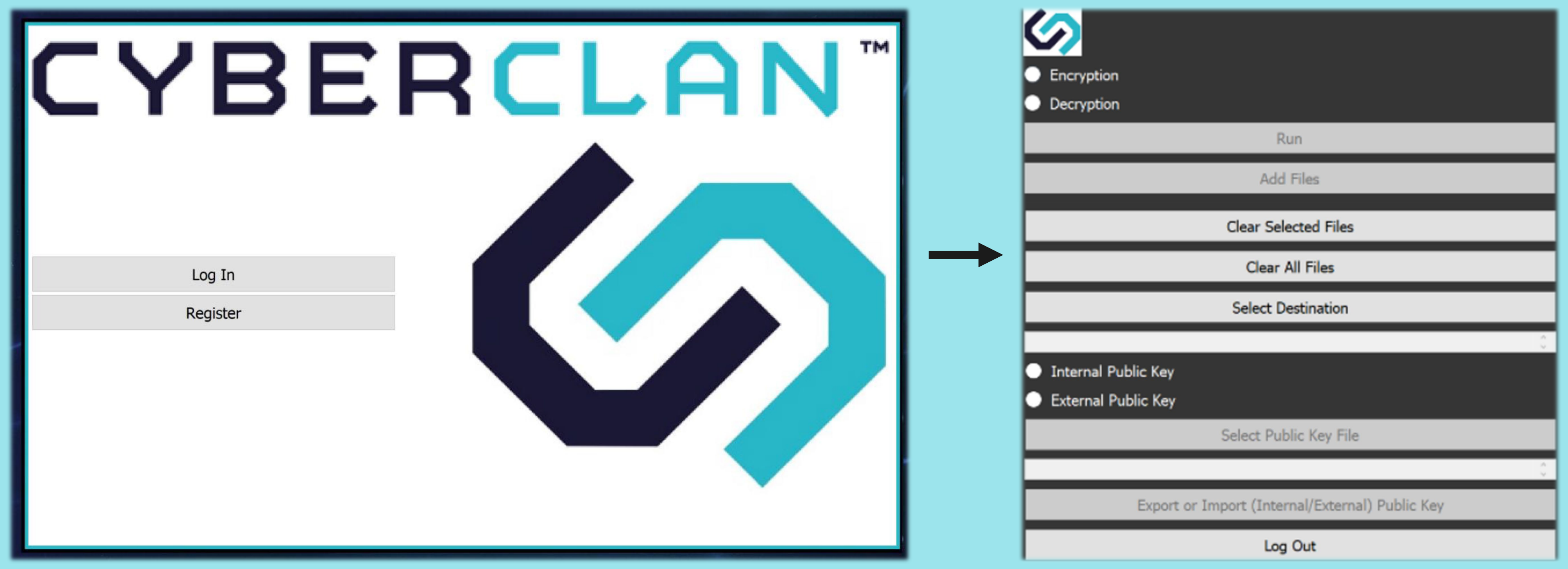
- GUI and PCB design were acquired from Phase 1 team.
- File encryption/decryption libraries have been acquired from STMicroelectronics (STM).
- Created C code for creating and logging into accounts.

Testing:

- Will test functionality of encryption, decryption, account login, and account creation.

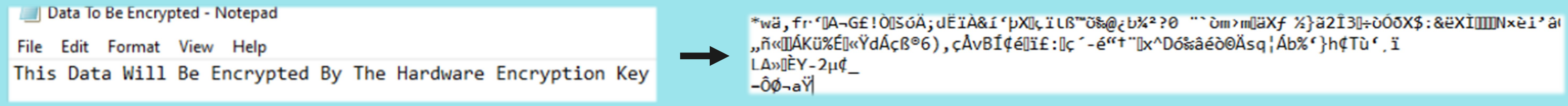
Details of Software Design

- When the HEK is plugged into a PC, the Graphical User Interface (GUI) will appear.
- The HEK will have multiple users able to encrypt/decrypt files, and each user will have an account.
- Each account has a username, password, and encryption keys that distinguish one account from another.
- User must log into account to be able to encrypt/decrypt files.
- Once logged in the user can choose whether to encrypt or decrypt a file, choose a specific file to encrypt or decrypt, and choose where they want the output file stored.



File Encryption:

- User logs into GUI account and selects file to be encrypted.
- File contents are encrypted using AES-256 (Advanced Encryption Standard-256 bit key).
- AES-256 key is put into file header.
- The user’s public RSA-4096 (Rivest-Shamir-Adleman-4096) key encrypts the AES-256 key.
- Now, the file has been encrypted and converted into ciphertext (shown below):



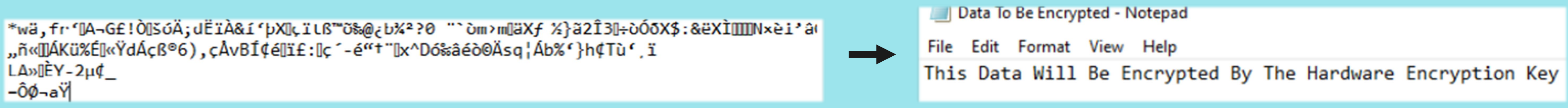
```
This Data Will Be Encrypted By The Hardware Encryption Key
```

```
*wä,fr·‘A¬G£!ÒŠóÄ;dËïÀ&í‘þXç‚ïlß™õ‰@¿b¾²?0 "`òm›mäXƒ ½}ä2Î3÷òÓðX$:&ëXÌNxèi’â
„ñ«ÁKü%É«ŸdÁçß®6),çÅvBÍ¢éï£:ç´-é“†¨x^Dó‰âéò©Äsq¦Áb%‘}h¢Tù‘.ï
LA»ÈY-2µ¢_
–Ôø¬aŸ
```

- User can choose to save encrypted file to HEK or to local PC.

File Decryption:

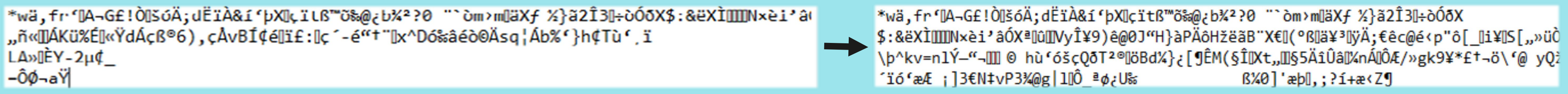
- User logs into GUI account and selects file to be decrypted.
- AES-256 key in file header is decrypted using the user’s private RSA-4096 key.
- AES-256 key decrypts the file contents to recover the original file (shown below):



```
*wä,fr·‘A¬G£!ÒŠóÄ;dËïÀ&í‘þXç‚ïlß™õ‰@¿b¾²?0 "`òm›mäXƒ ½}ä2Î3÷òÓðX$:&ëXÌNxèi’â
„ñ«ÁKü%É«ŸdÁçß®6),çÅvBÍ¢éï£:ç´-é“†¨x^Dó‰âéò©Äsq¦Áb%‘}h¢Tù‘.ï
LA»ÈY-2µ¢_
–Ôø¬aŸ
```

```
This Data Will Be Encrypted By The Hardware Encryption Key
```

- Since each user has a unique RSA-4096 private key, if another user attempts to decrypt the file the original file will not be recovered (shown below):

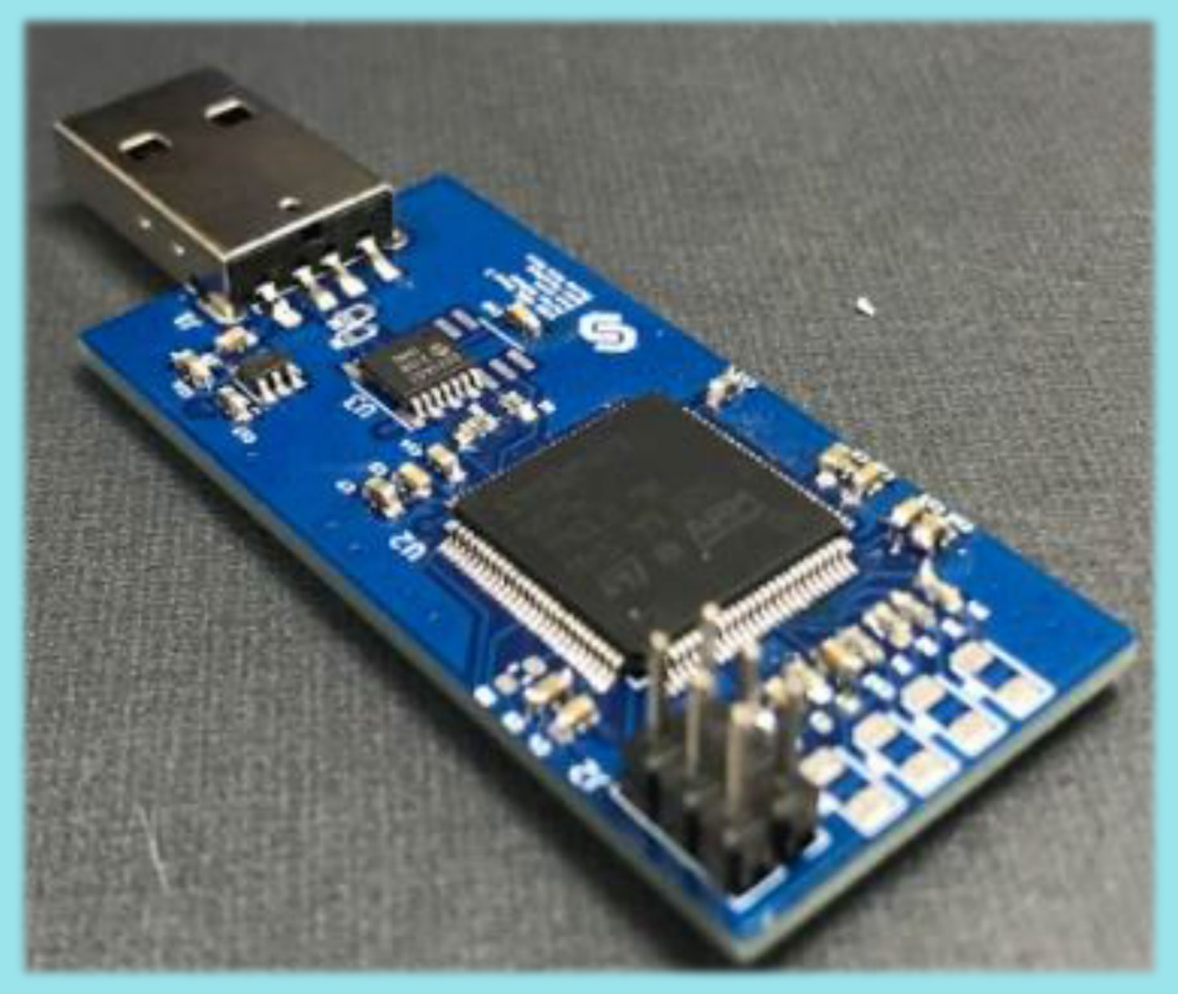


```
*wä,fr·‘A¬G£!ÒŠóÄ;dËïÀ&í‘þXç‚ïlß™õ‰@¿b¾²?0 "`òm›mäXƒ ½}ä2Î3÷òÓðX$:&ëXÌNxèi’â
„ñ«ÁKü%É«ŸdÁçß®6),çÅvBÍ¢éï£:ç´-é“†¨x^Dó‰âéò©Äsq¦Áb%‘}h¢Tù‘.ï
LA»ÈY-2µ¢_
–Ôø¬aŸ
```

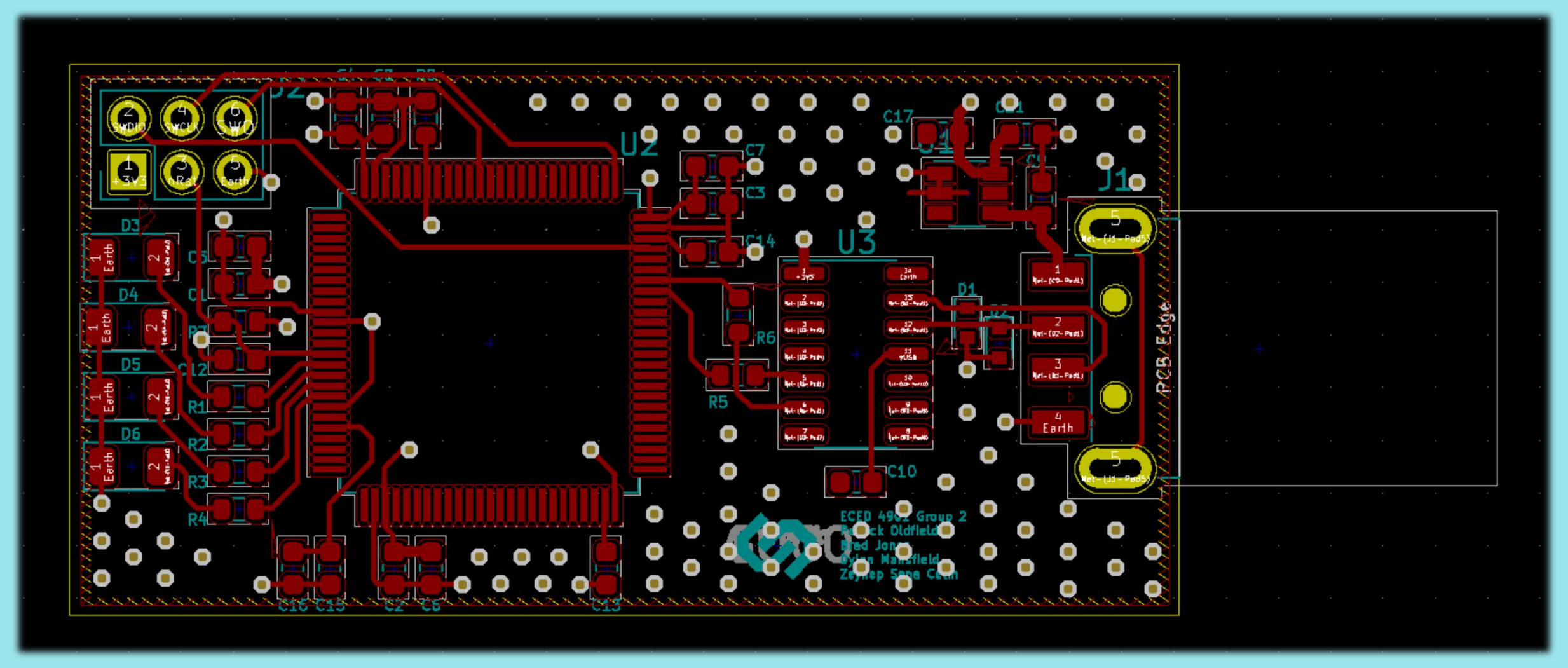
```
*wä,fr‘A¬G£!ÒŠóÄ;dËïÀ&í‘þXçïtß™õ‰@¿b¾²?0 "`òm›mäXƒ ½}ã2Î3÷òÓðX
$:&ëXÌNxèi’âÓXªûVyÎ¥9)ê@0J“H}àPÄõHžëãB¨X€(°ßä¥³ÿÄ;€êc@é‹p"ô[_i¥S[„»üÒ
\þ^kv=nlÝ–“¬ © hù‘óšçQðT²®öBd½}¿[¶ÊM(§ÎXt„§5ÄîÛâ¼nÁÔÆ/»gk9¥*£†¬ö\‘@ yQ
´ïó‘æÆ ¡]3€N‡vP3¾@g|1Ô_ª¢¿U‰ ß%0]'æþ,;?í+æ‹Z¶
```

- User can select to save decrypted file to HEK or to local PC.

Details of Hardware Design



- STM32H757 microcontroller to be used:
  - 2MByte flash memory for storing GUI and encryption code and account information.
  - Speeds up to 240MHz.
  - Has AES accelerator to speed up encryption/decryption using AES-256.
- USB-A port to be used for connection to user’s workstation.
- External flash memory chip will be dedicated to storing encrypted/decrypted files.
- HEK will use custom designed PCB (shown below):



Conclusion and Recommendations

- We would like to thank Richard D’Souza and Dr. Larry Hughes for their continual support.
- The team needs to investigate additional flash memory chip for dedicated file storage.
- PCB may need to be redesigned to accommodate additional memory chip.
- GUI code needs to be run off HEK – is currently running off user’s PC (currently not portable).
- Need to incorporate C account login code into GUI software.
- For more information on CyberClan, visit https://cyberclan.com/.