Name: MIDN 2/C Eshleman

Course / Section: SY303 /3321

Enclosures: Completed Version of AsmProject.s

**RUBRIC**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section** | **0%** | **50%** | **80%** | **100%** | **Max Points** |
| Used Template | No | Partially |  | Yes | 10 |
| Procedure | Discussed procedure could not be reproduced | Some steps and tools missing | Progressing | Comprehensive and clear | 10 |
| Results | Not present or not discussed | Incorrect results without explanation | Progressing | Correct, well-explained results | 15 |
| Discussion | Questions not answered or answers are off-topic. | Discussions lack complete consideration. Terse responses. | Progressing | Well-developed discussions with interesting insights | 30 |
| Asm Code | Missing or not commented | Incomplete, has errors, missing name or comments | Progressing | Includes identification and clear descriptions of all code | 20 |
| Keil Emulator Screenshots | Missing | Does not capture full simulator screen or wrong | Progressing | All present, shows status of test script, full legible screen capture | 10 |
| Grammar/Professionalism | Poor grammar and/or unprofessional language |  | Progressing | Professional writing | 5 |

**SCENARIO:**

**(USNA) Mission Overview**

(USNA) Army week is coming up and COVID-19 has made tensions are higher than ever. The cadets have already paraded their mule down Stribling Walk and defaced Tecumseh. And they weren’t even wearing masks!! Your company officer has made you responsible for having Army week run smoothly and without incident or she will **place you in an extended ROM status in Bancroft Hall through winter break**. Your mission is to figure out what your adversary is planning and put a stop to it. We’re all counting on you!

(USNA) Luckily, a hardware device has been swiped from an exchange cadet that happens to

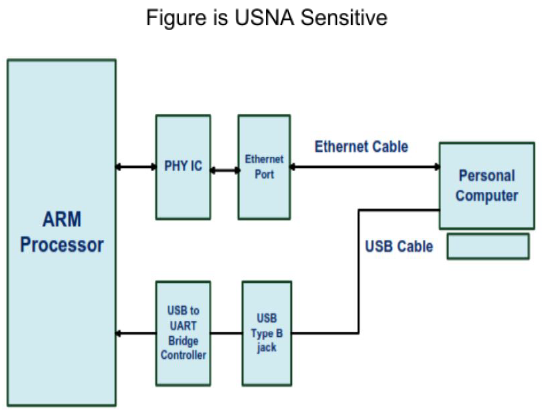
be an ARM Cortex M3 NXP LPC1768 based embedded device. It allowed him to communicate back to Westpoint and plan the dastardly deed. The captured device when executed has messages encrypted and stored in memory. You will need to decrypt the message and send it to an analyst for interpretation.

(USNA) The ARM Cortex M3 processor is instrumental in coordinating the actions of our

Westpoint adversaries. If we can decode and exfiltrate (EXFIL) the messages out of the

network to our forces that will help safeguard Army week. Figure 1 illustrates the adversarial

network [1] the detailed schematic is illustrated in figure 2 [1].



**(USNA) Figure 1**: Integration of the ARM Processor and the importance of adversarial

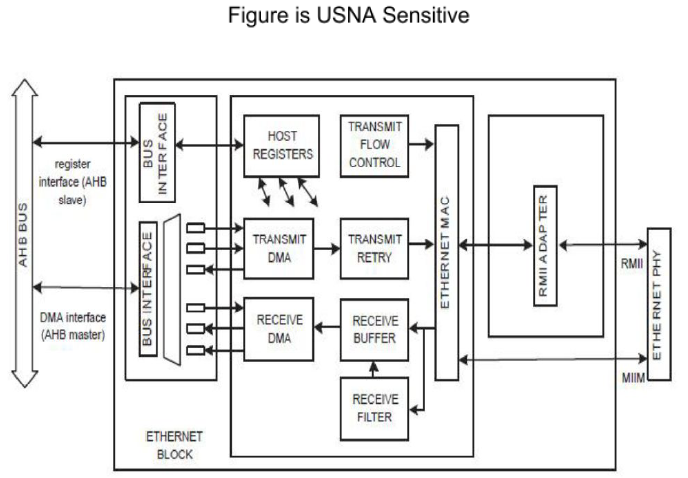
communications [1].

(USNA) A **covert channel** is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. (wikipedia)

(USNA) Reading the registers and then encoding the light sequence would give us the

information advantage to foil any plans the cadets attempt to execute, giving us the upper hand

in morale for the big game. Discover their plot and make Mother B proud!



**(USNA) Figure 2**: Schematic of a futuristic ethernet communications device [1].

**(USNA) Operational Needs Statement - Exploitation and EXFIL Requirements**:

1. (USNA) Access the memory stored in the data registers prior to being overwritten

2. (USNA) Crack the encryption key

3. (USNA) Identify the language encoding set that is being used

4. (USNA) Decode the message from the encoding set

5. (USNA) Decrypt the message and thwart the Army plan

(USNA) Additionally, you were able to get your plebes to do recon in the exchange cadets’ room

to gather some useful intelligence. MIDN 4/C Namath was able to find the secret key scheme

that could be used to decrypt the memory registers to reveal the encoded characters (consider

known character encodings). It turns out that the encrypted bitstream is stored in the R0 register whenever LED2 is illuminated and the bits for the key to decrypt the ciphertext is gathered from the least significant bit of the R0 register whenever LED4 is lit. He is just in plebe cyber and has NO IDEA what this means. Luckily, you are an experienced Cyber Operations major and will have this case cracked in no time! Happy Hacking!

**(USNA) Secret Key**

(USNA) The secret key was EXFIL-ed over secure communications to your device over 32 occurrences of the R0 least significant bit. Join them into one 32-bit value.

References:

[1] Kavya M.P., Thanuja T.C., Angadi N.G., “Development of a Prototype for Ethernet Port With ARM Cortex-M3 Processor for Web Applications” International Journal of Research and Technology Vol. 4., Issue 9, September 2015

**PROCEDURE:**

What did you do in the project? What steps did you take to accomplish your objective in general?

For the first part of the project we had to initialize the LED’s for the output of the GPIO. Then we set R1 to the base address of the GPIO for the desired LEDs which is the hex value of 0x00B40000 which means all four LEDs will turn on. Then we store the LEDs GPIO to output by zero by storing this value into the GPIO direction register. The next portion of the project that we needed to accomplish was to find the encrypted key. We know that when LED 4 is lit up that the encrypted key is stored in R0.

So we ran through the code and every time LED 4 lit up we copied down the hex value that is stored in R0. After the LED lit up 32 times we know that the key is the least significant bit. So we had to convert all 32 hex values into binary and copy down the least significant bit for each. After this process we get 32 bits of information. Then we put that value back into our programming calculator and we get the hex value of **0x72C2EE9D** which is the decryption key used. Once we find this value we then code it into the AsmProject code. We need to update the value of R7 to the decryption key using MOV32. Once this is coded we now need to run through the code and see when LED 2 lights up.

Every time LED 2 lights up that is the message we are trying to find stored in R0. We know that this is now the message because we have now put our decryption key into the code. We then run through the program and copy down the value of R0 everytime LED 2 is lit. This results in 32 hex values that we can use as the decrypted message. Then we must take all of the hex values and convert them into ASCII characters, once this is done we get the secret message.

**Secret Message:** Hua, Hua, HUA! We will kidnap Bill the Goat on Friday night @ 2100 as he is escorted out of USNA thr Gate 3. HUA, HUA, HUA!!

**RESULTS:**

The decryption key is 0x72C2EE9D

**Secret Message:** Hua, Hua, HUA! We will kidnap Bill the Goat on Friday night @ 2100 as he is escorted out of USNA thr Gate 3. HUA, HUA, HUA!!

Who is the target? Bill the Goat

When is the operation going down? Friday night @ 2100

Where should we send reinforcements? Gate 3

**DISCUSSION (For these questions you may seek quality information from the internet or other resources.  Be sure to cite all sources used for research, give the exact URL(s) visited):**

1. **Research and describe how different materials and processes are required to make different LED colors. What is something about the development of LEDs that surprised you? An LED is a semiconductor light source that emits light when current flows through it. Electrons in the semiconductor recombine with electron holes, releasing energy in the form of photons. The color of the light (corresponding to the energy of the photons) is determined by the energy required for electrons to cross the band gap of the semiconductor. I was surprised that LED’s are so complex. They make them run and change colors, I thought they were simply made to produce a single color.**

[Light-emitting diode](https://en.wikipedia.org/wiki/Light-emitting_diode)

[LEDs and OLEDs](https://edisontechcenter.org/LED.html)

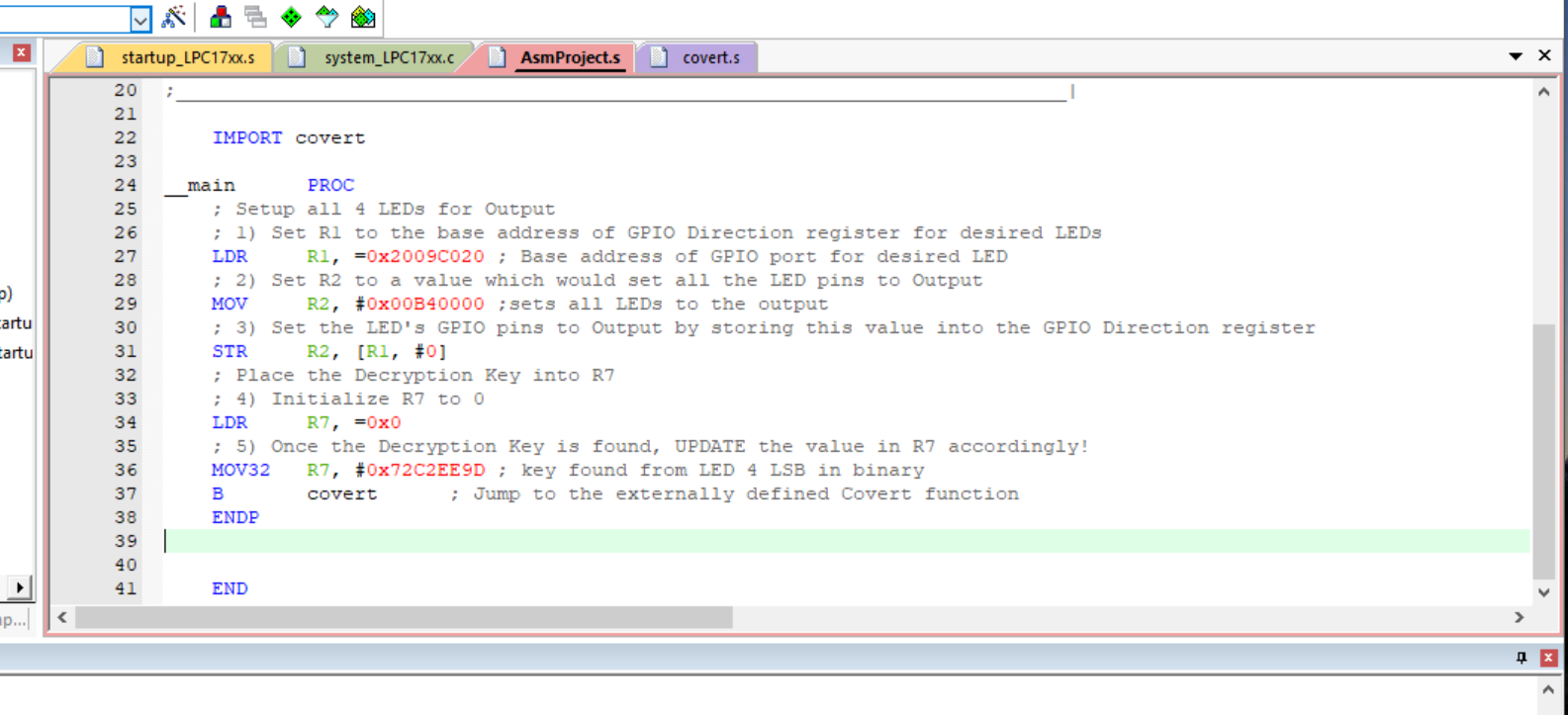
1. **Section 8.4 of the manual describes the Pin Mode register and how it can be used to tie a pull-up or pull-down resistor (or neither) to a GPIO pin. What are the functions of these resistors? How are they used for instance if using the pins for serial communication? The pull-up or pull-down resistor can be selected for every port pin regardless of the functions on the pin. These resistors are used to control the mode of a port pin, two in a PINMODE register, and an additional one in PINMODE\_OD register. The PINMODE\_OD refers to the open drain mode for ports, it causes the pin to be pulled low normally if it is configured as an output and the data value is a 0. If the data value is a 1, the output drive of the pin is turned off, equivalent to changing the pin direction. This combination simulates an open drain output.**
2. **Part of your analysis in this project was determining what encryption mechanism was in use. Is this function used for encryption of real-world data? What makes it so prevalent in encryption algorithms? You should discuss the unique properties stemming from the truth table of this function and how the function facilitates encryption and decryption successfully given the correct key.**

**For the encryption used in this project we found the key from the least significant bits stored in the LED 4 R0 register. Once we found our decryption key then we stored it in the location register of R7. In the convert code the R7 is used with a EOR command. This method of encryption uses the Hamming distance, which is the number of bit positions in which two bits are different. This is what gives us the value of R0 when LED 2 is lit up.**

**COMMENTS:**

I thought this project was really fun and reminded me of the microcorruption engagement points. It was like a puzzle trying to solve for the message and I felt like it was for a purpose and not just coding random things. This was a tedious project but I thought it was worth it.

**ENCLOSURE (1): Completed Version of AsmProject.s**

****