SCHOOL OF ELCTRICAL ENGINEERING

FACULTY OF ENGINEERING

UNIVERSITI TEKNOLOGI MALAYSIA

20222023 - 1

SEEL 5123 – 01 / MKEL 1123 – 01

PROJECT PROPOSAL

GROUP 2

Implementation of AES Algorithm in Blue Pill (STM32F103C8T6)

1 ZHANG ZHEN

2 TIAN LINXUE

3 LIM ZHI

1) Introduction

AES (Advanced Encryption Standard) is a widely used symmetric encryption algorithm that is used to protect data in various applications. It is used in data encryption, network security, online communications, digital rights management, military and government applications, and many other areas where data security is important. AES is considered to be a highly secure encryption standard, and is used by many large organizations, government agencies, and other entities around the world. The popularity of AES is due to its strong encryption capabilities, compatibility with a wide range of devices and systems, and widespread availability of implementation libraries. Overall, AES is an essential tool for protecting sensitive information and ensuring the security and privacy of digital data. This paper introduces an implementation of AES encryption algorithm on the STM32 Blue Pill microcontroller. Encryption may be done using a computer that has AES algorithm on it, and since a computer is exposed to be hacked, our proposed microcontroller will help users to overcome this problem. Thus, users can use the AES build in algorithm to encrypt their data on a computer using a USB that connects the microcontroller to the computer and encrypt using symmetric encryption. In this project, we use an analogue sensor to replace the computer which is used to provide the input data for the encryption purpose.

2) Proposed Methodology

AES operates on 128-bit blocks of data using different size secret keys depends on the desired security level [1] . It can divide into four basic operation blocks which are byte substitution, rows shifting, mix columns and key addition.

I. Byte substitution: substitution function using a nonlinear byte substitution table (S-BOX).
II. Shift Row: permutation function that shift byte cyclically to the left.
III. Mix Column: encryption/decryption process and key generation process using Galois Field.
IV. Key Addition: XOR each byte of state and round key.

For the encryption, an initial add round key operation proceeds the first round. Then each operation will be loop for 9 rounds with different round key. The final round repeats the same previous loop except mix columns operation.

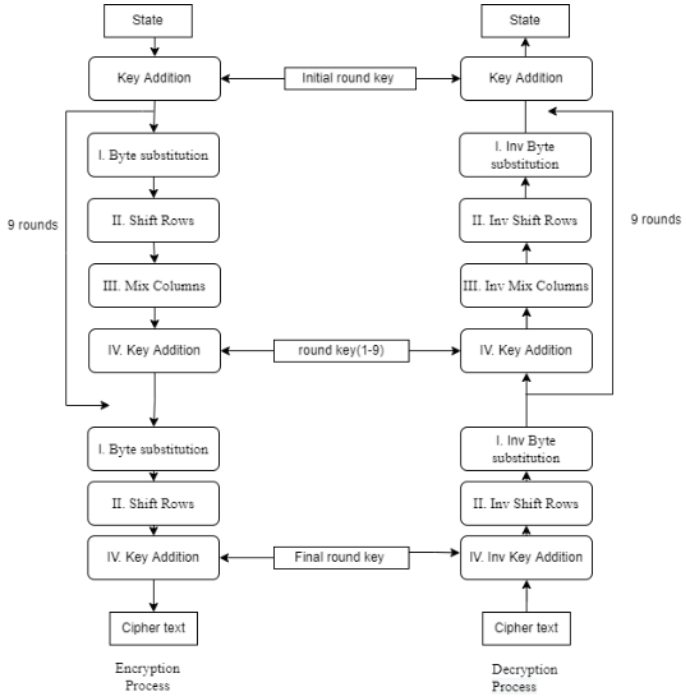

Figure 1: Encryption and decryption algorithm

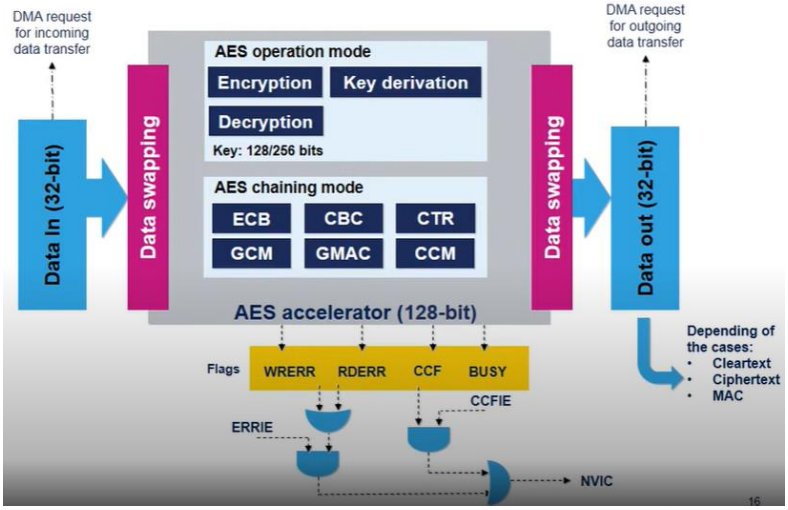

Figure 2: AES system Architecture

Meanwhile, for decryption process, it uses the inverse functions of each operation with the reversed key arrangement that starts with the final round key [2]. All steps are concluded in Figure 1.

3) Hardware Involved

In this project, we are using a 32-bit ARM Cortex-M3 processor, STM32F103C8T6 board which has a maximum clock speed of 72 MHz and includes 64 kilobytes of flash memory and 20 kilobytes of SRAM. This microcontroller also features a wide range of peripherals, including timers, USARTs, SPI, I2C, and more, making it suitable for a variety of applications. This board has a build-in cryptographic acceleration module called Hardware Crypto Processor (HCP) which provided hardware acceleration for AES encryption and decryption. Besides, an analog digital convertor (ADC) port is needed to receive the analog input and concert to digital data for the encryption process. In addition, a I2C port is also needed by OLED screen for the displaying purpose. The data that is decrypted can displays on the OLED screen.

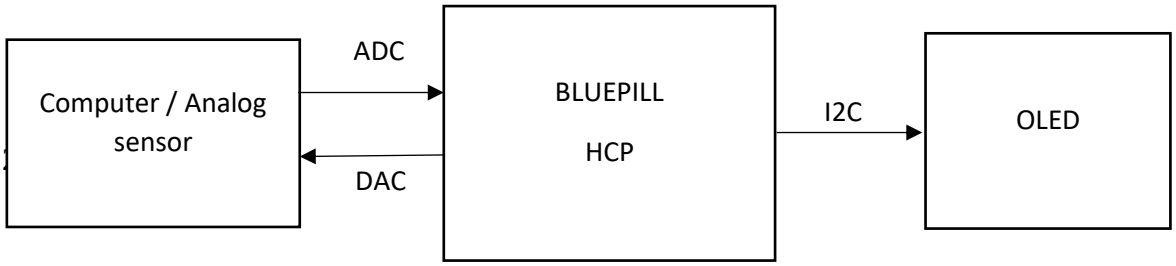

Figure 3: Block diagram of the system

4) Software Involved

The program is written and programmed using STM32CubeIDE. Several software libraries to fully utilize STM32 capabilities are expected to be involved in this project [3].

I. CMSIS - Core(M): To access the processor core, device peripherals of Cortex-M devices.
II. CMSIS - Driver: To receive and transmit data by USART.
III. CMSIS - RTOS: To enable flexible scheduling of system resources offers methods to communicate between threads.
IV. CMSIS - SVD/DAP: To access in-circuit debugging.
V. STM32Cube HAL Cryptographic: To access the Hardware Crypto Processor (HCP) for AES encryption or decryption.

5) Conclusion

Since it is implemented on a 32-bit processor, it is expected to get a better performance than the original 8-bit microcontroller. The operation time and CPU cycle of encryption and decryption operation will be compared to ATmega644p [1]. Hence, STM32 Blue Pill a good choice for applications that require high-speed encryption and decryption.

6) References

[1] H. Lee, K. Lee, and Y. Shin, “AES Implementation and Performance Evaluation on 8-bit Microcontrollers,” vol. 6, no. 1, pp. 70–74, 2009.

[2] A. E. T. El_Deen, “Implementation of AES Algorithm in MicroController Using PIC18F452,” *IOSR J. Comput. Eng.*, vol. 15, no. 5, pp. 35–38, 2013, doi: 10.9790/0661-1553538.

[3] https://arm-software.github.io/CMSIS_5/General/html/index.html

[4] https://wiki.st.com/stm32mcu/wiki/Security:Introduction_to_the_cryptographic_library_with_STM32