AES256IP Demo Instruction

Rev1.02 29-Aug-2022

This document describes the instruction to demonstrate the operation of AES256IP on ZCU106 Evaluation Board. In the demonstration, AES256IP are used to encrypt and decrypt data between two memories in FPGA. User can fill memory with plain or cipher data patterns, set encryption/decryption key and control test operation via serial console.

1 Environment Setup

To operate AES256IP demo, please prepare following test environment.

1) FPGA development boards (ZCU106 board).
2) Test PC.
3) Micro USB cable for JTAG connection connecting between ZCU106 board and Test PC.
4) Micro USB cable for UART connection connecting between ZCU106 board and Test PC.
5) Vivado tool for programming FPGA installed on Test PC.
6) Serial console software such as TeraTerm installed on PC. The setting on the console is Baudrate=115,200, Data=8-bit, Non-parity and Stop=1.
7) Batch file named “AESIPTest_ZCU106.bat (To download these files, please visit our web site at www.design-gateway.com)

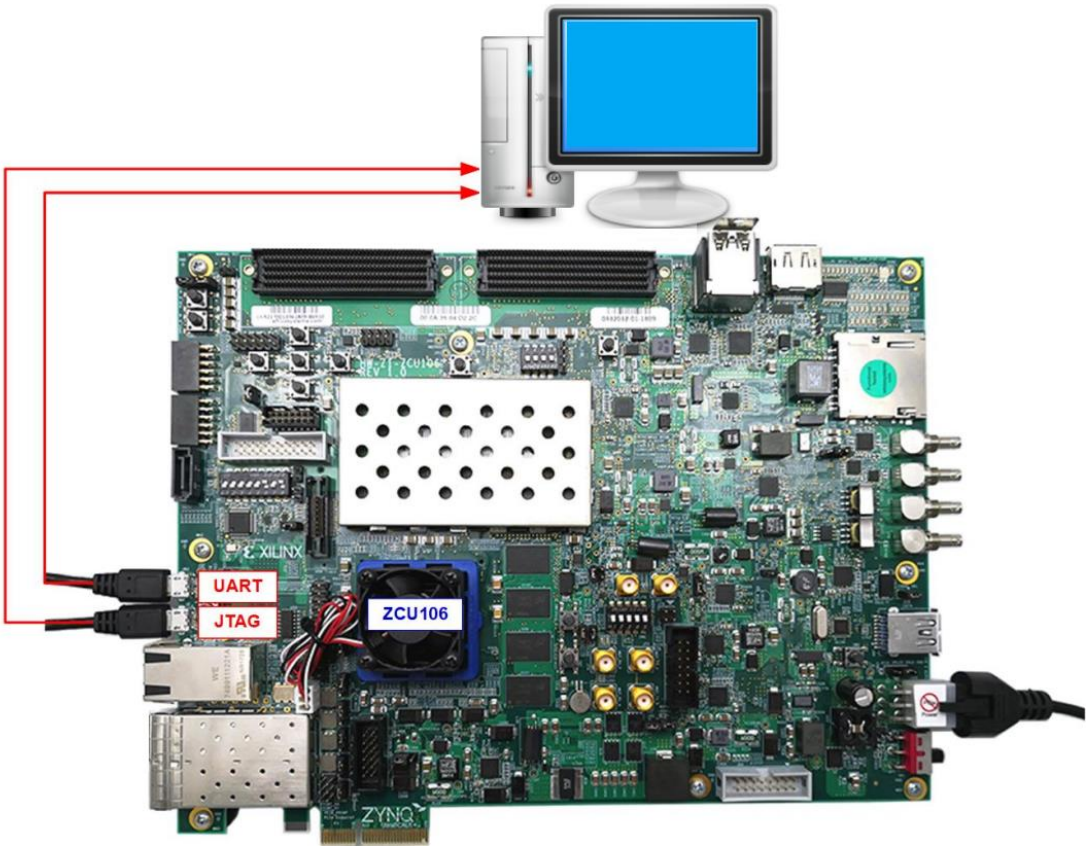

Figure 1-1 AES256IP demo environment on ZCU106 board

2 ZCU106 board setup

1) Make sure power switch is off and connect power supply to FPGA development board.
2) Connect two USB cables between FPGA board and PC via micro-USB ports.
3) Power on system.
4) Download configuration file and firmware to FPGA board by following step,
    a) open Vivado TCL shell.
    b) change current directory to download folder which includes demo configuration file.
    c) Type “AESIPTest_ZCU106.bat, as shown in Figure 2-1.

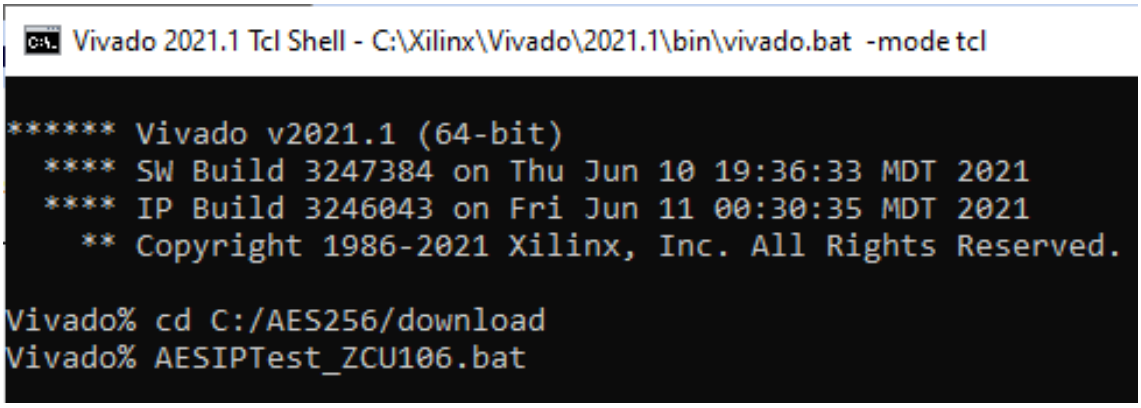

Figure 2-1 Example command script for download configuration file

3 Serial Console

User can fill RAMs with plain or cipher data patterns, set encryption/decryption key and control test operation via serial console. When configuration is completed, AES256demo command menu will be displayed as shown in Figure 3-1. The detailed information of each menu is described in topic 4.

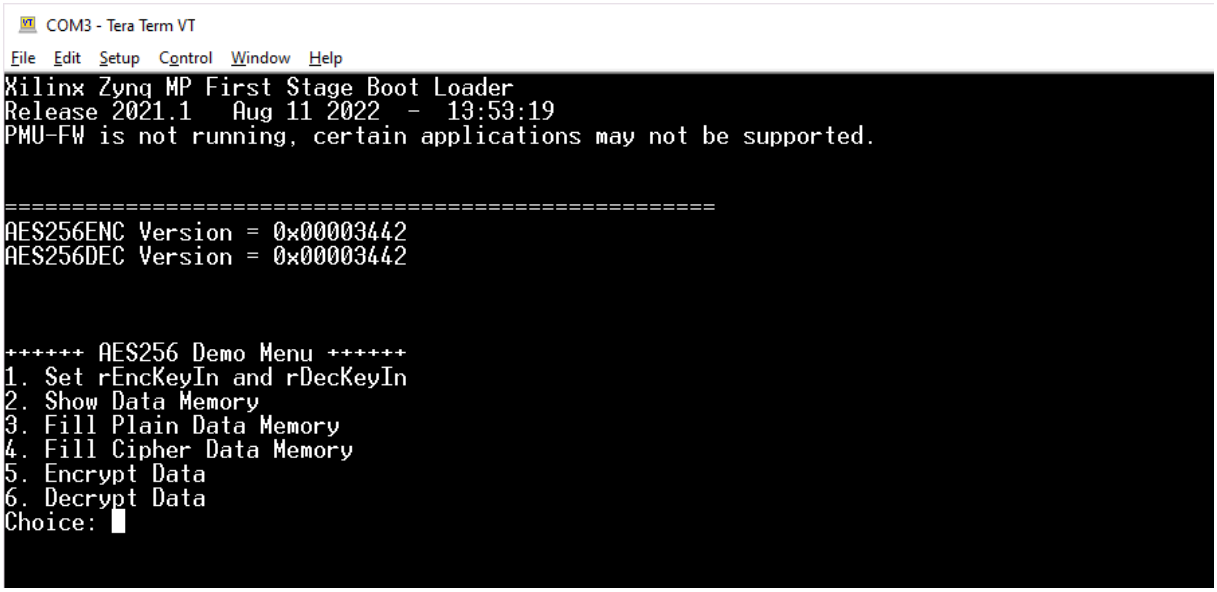

Figure 3-1 Serial console

4 Command detail and testing result

4.1 Set encryption/decryption key

Step to set encryption key and decryption key as follows

a) Select “1. Set rEncKeyIn and rDecKeyIn”.
b) Current encryption key will be displayed on serial console as shown in Figure 4-1.
c) Set new encryption key: User is allowed to input new key in hex format or press “enter” to skip setting new key. Then the current encryption key is printed again.
d) Current decryption key will be displayed on serial console.
e) Set new decryption key: User is allowed to input new key in hex format or press “enter” to use rEncKeyIn as rDecKeyIn. Then the current decryption key is printed again.

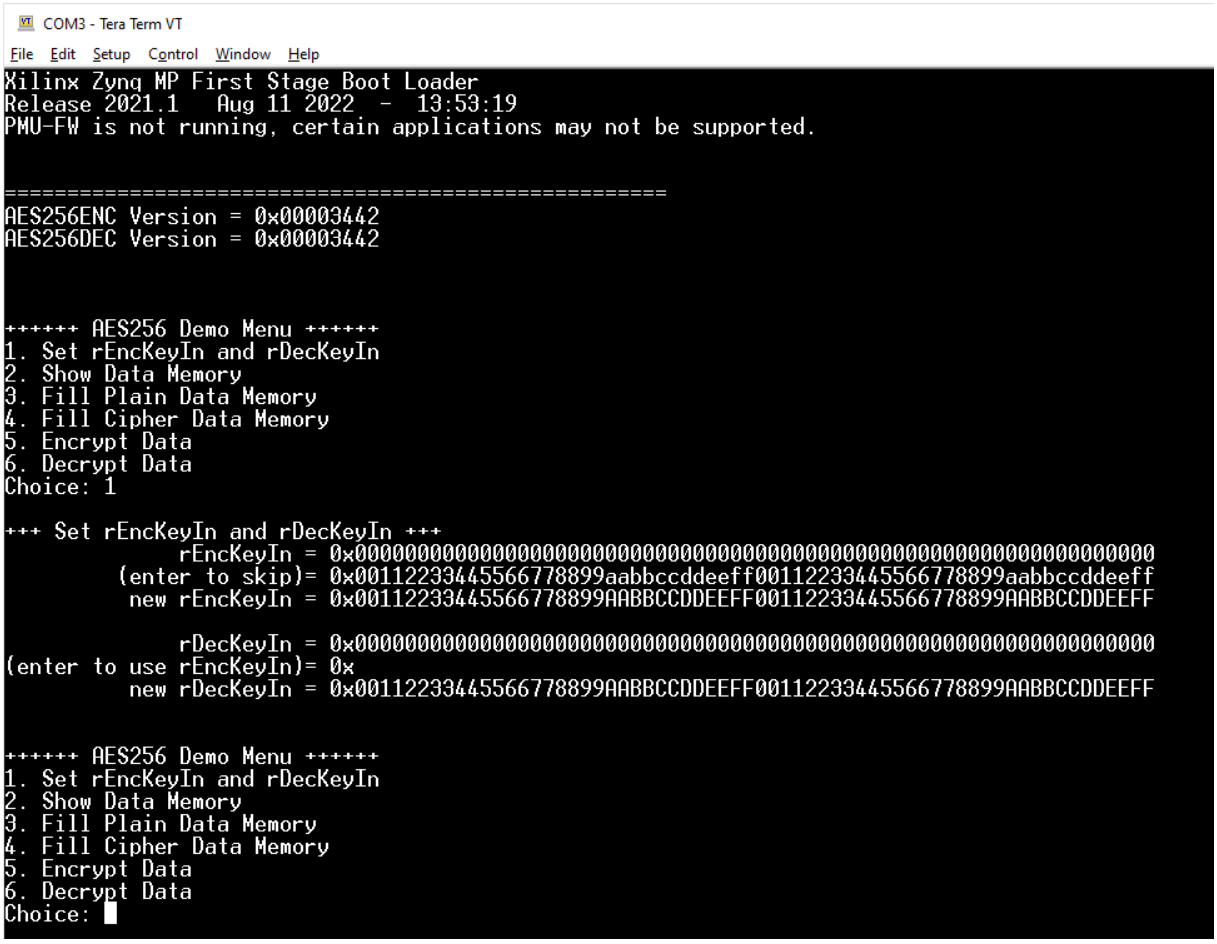

Figure 4-1 Set rEncKeyIn and rDecKeyIn example

4.2 Show Data Memory

To show data in memory, user can select “2. Show Data Memory” and input the desired number of 128-bit data to show. Both plain data and cipher data will be displayed in table-form as shown in Figure 4-2. User can press “enter” key to skip putting the number of data, then serial console will display five rows of 128-bit plain data and 128-bit cipher data at address 0x0000-0x004F.

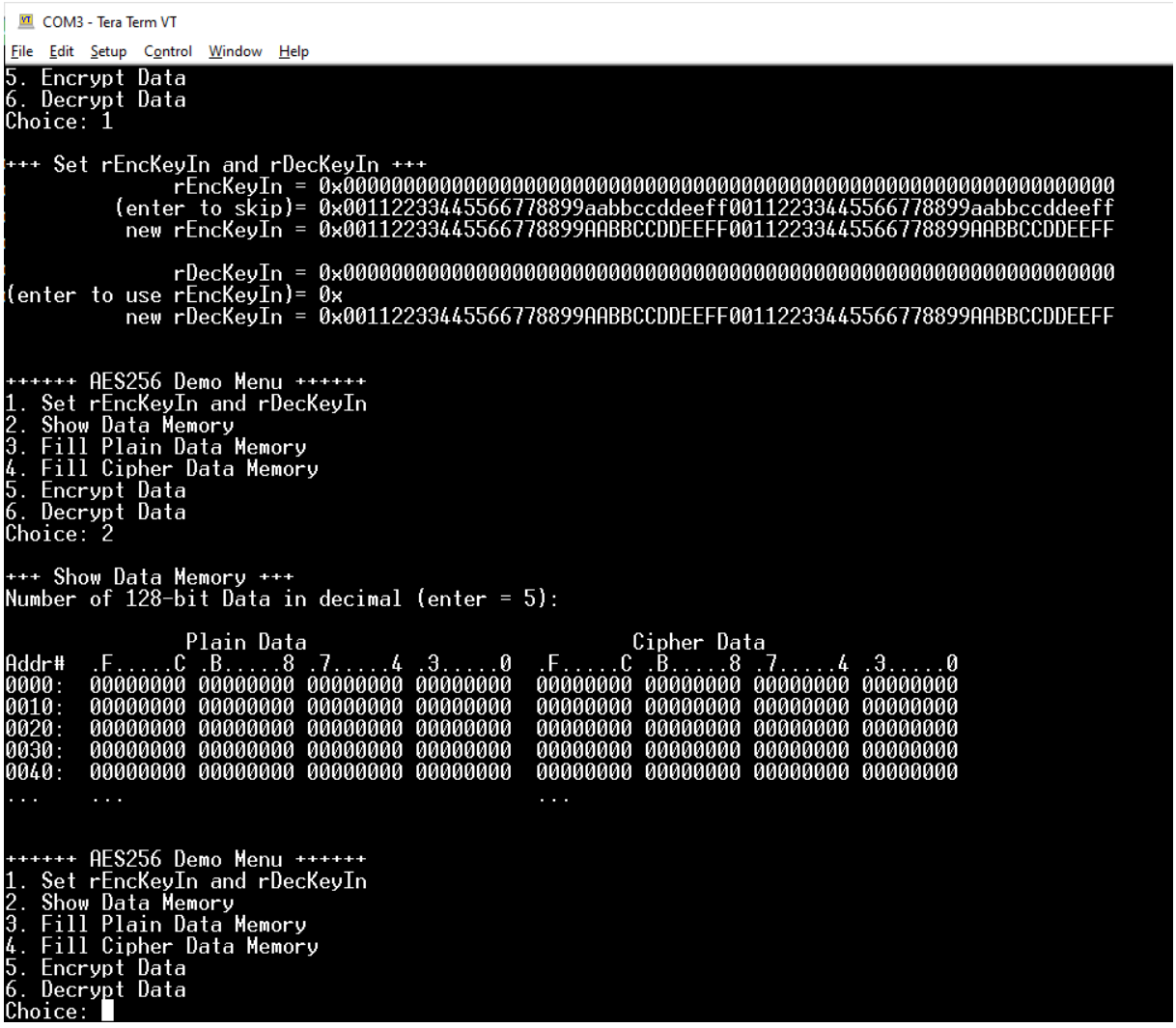

Figure 4-2 Displayed Data when press “enter” key

4.3 Fill Plain Data Memory

Step to fill plain data in memory as follows

a) Select “3. Fill Plain Data Memory”.
b) There are four pattern to fill memory.
    a. zero pattern
    b. 8-bit counter
    c. 16-bit counter
    d. 32-bit counter
c) Whole plain-data memory is filled with selected data pattern.

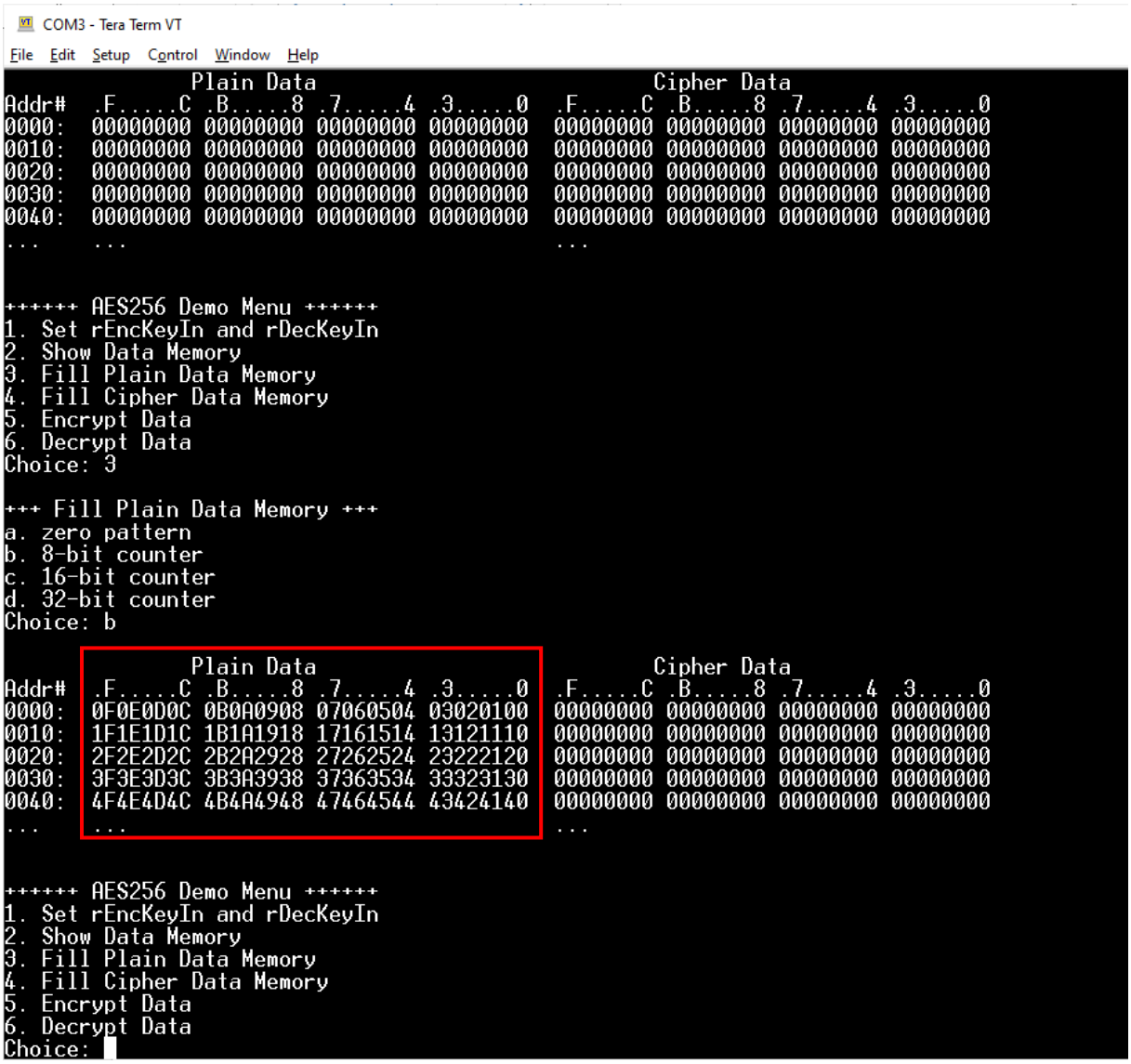

Figure 4-3 Displayed Data when select pattern b

4.4 Fill Cipher Data Memory

Step to fill Cipher data in memory as follows

a) Select “4. Fill Cipher Data Memory”.
b) There are four pattern to fill memory.
    a. zero pattern
    b. 8-bit counter
    c. 16-bit counter
    d. 32-bit counter
c) Whole cipher-data memory is filled with selected data pattern.

In this example, choice c is selected. DpRam2 is filled with 16-bit counter pattern and five rows of data in memories are displayed as Figure 4-4.

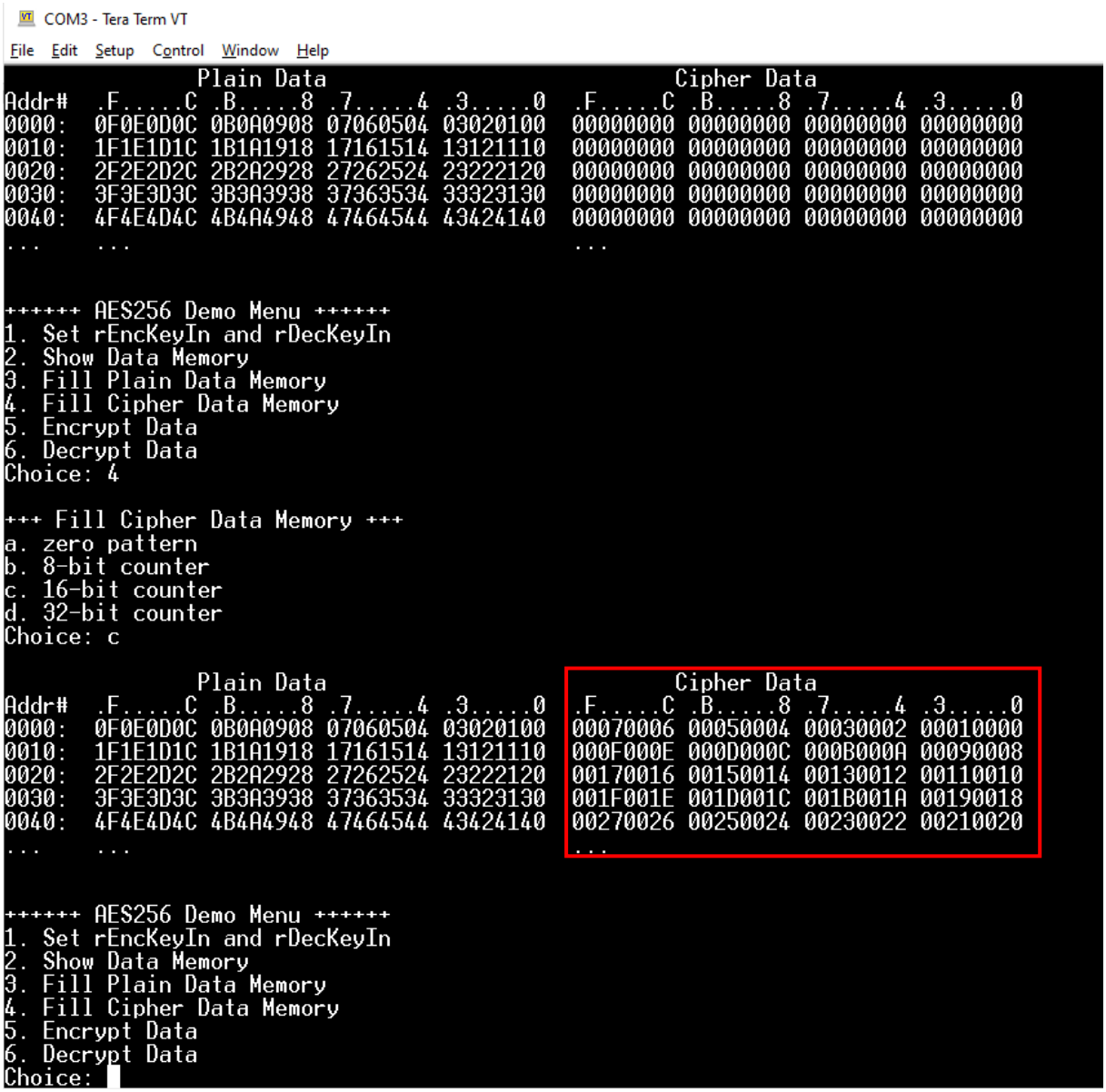

Figure 4-4 Displayed Data when select pattern c

4.5 Encrypt

Select “5. Encrypt” to encrypt plain data in memory. User can input the desired number of plain data to encrypt or press “enter” key to encrypt five 128-bit plain data. When the encryption process is finished, DpRam2 will be filled with cipher data from AES256ENC.

In this example, Number of 128-bit Plain Data was ‘5’ (default value). When AES256ENC finished encryption process, five rows of plain data and cipher data were displayed on serial console as shown in Figure 4-5.

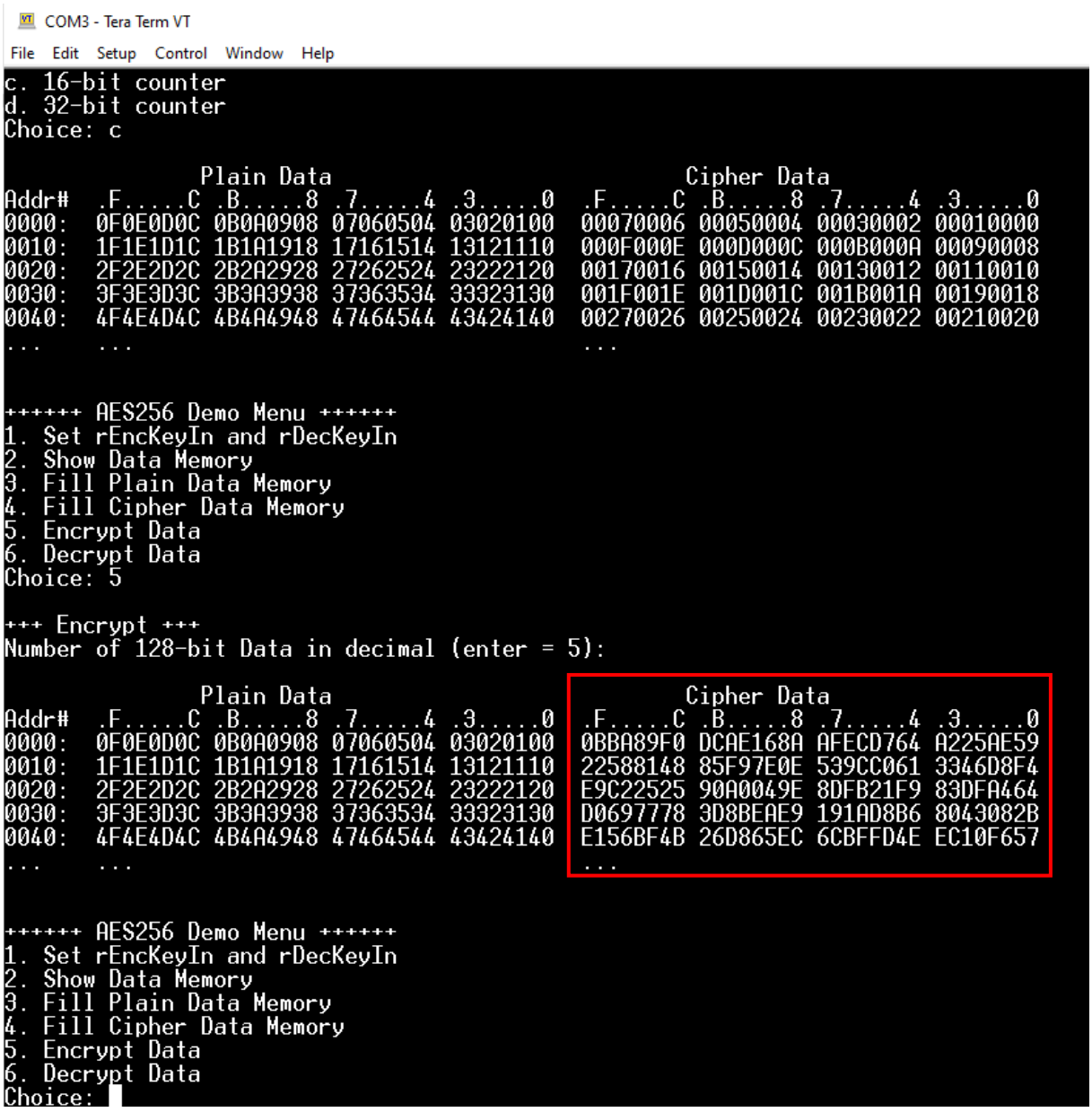

Figure 4-5 Serial console after finished encryption process

4.6 Decrypt

Select “6. Decrypt” to decrypt cipher data in memory. User can input the desired number of cipher data to decrypt or press “enter” key to decrypt five 128-bit Cipher data. When the decryption process is finished, DpRam1 will be filled with plain data from AES256DEC.

In this example, Number of 128-bit Cipher Data was ‘5’. When AES256DEC finished decryption process, five rows of plain data and cipher data were displayed on serial console as shown in Figure 4-6.

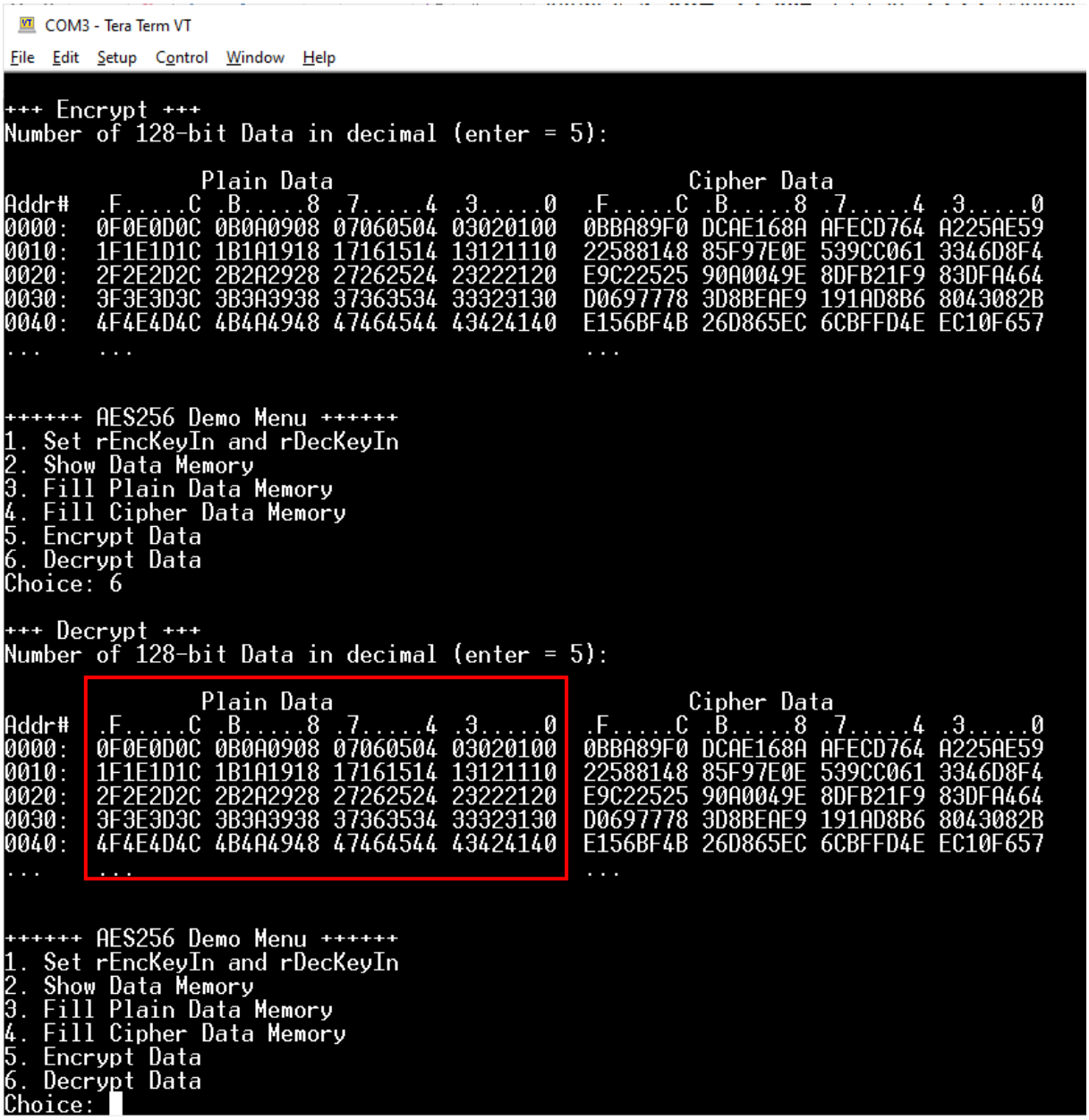

Figure 4-6 Serial console after finished decryption process

5 Revision History

Revision	Date	Description
1.00	7-Apr-2022	Initial version release
1.02	29-Aug-2022	Update description for new design