AES256XTS IP Demo Instruction

AES256XTS IP Demo Instruction

Rev1.00 2-Jun-2023

This document describes the instruction to demonstrate the operation of AES256XTSIP on FPGA development boards. In the demonstration, AES256XTSIP are used to encrypt and decrypt data between two memories in FPGA. User can fill memory with plain or cipher data patterns, set encryption key, tweakable key, Initialization Vector (IV) and control test operation via Nios II Command Shell.

1 Environment Setup

To operate AES256XTSIP demo, please prepare following test environment.

1) FPGA development board
   - Agilex F-series development kit. or
   - Arria10 SoC Development board.
2) Test PC.
3) Micro USB cable for JTAG connection connecting between FPGA boards and Test PC.
4) Quartus programmer for programming FPGA and Nios II command shell, installed on PC.
5) SOF file named “AES256XTS.sof” (To download these files, please visit our web site at www.design-gateway.com)

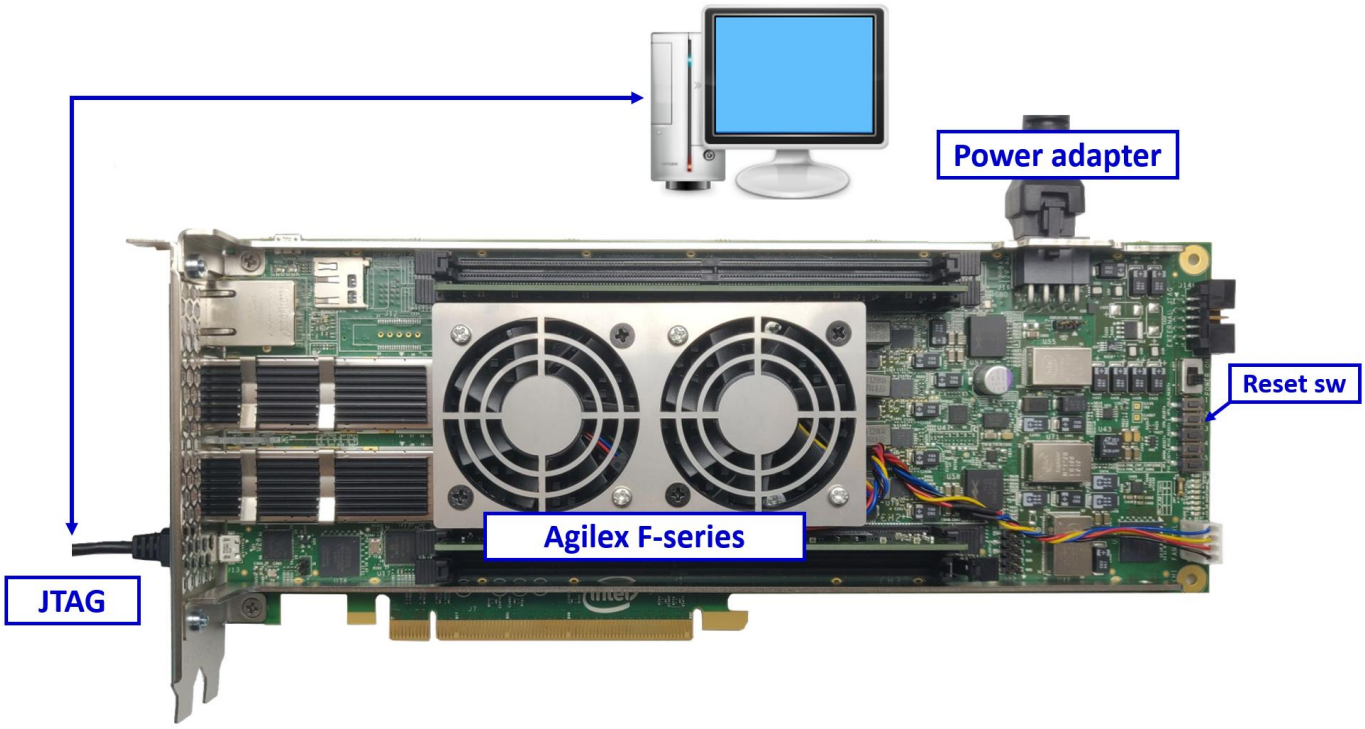

Figure 1-1 AES256XTSIP demo environment on Agilex F-series board

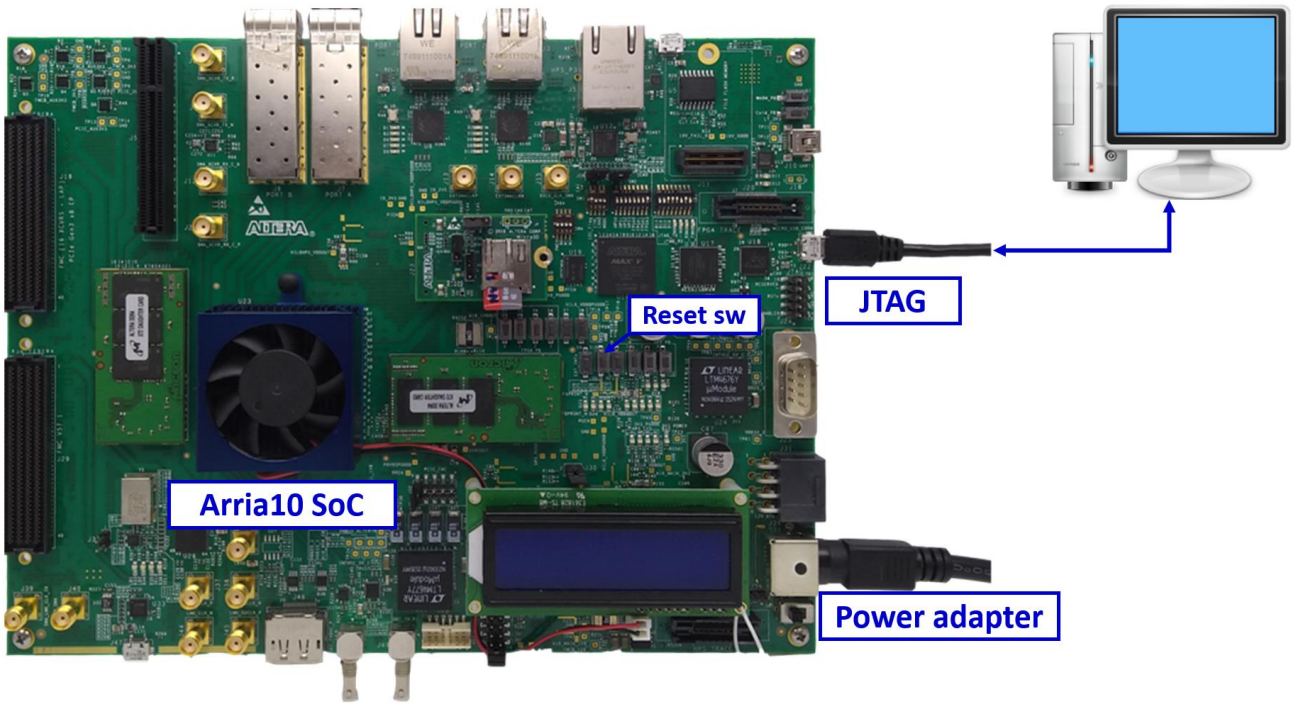

Figure 1-2 AES256XTSIP demo environment on Arria10 SoC board

2 FPGA development board setup

1) Make sure power switch is off and connect power supply to FPGA development board.
2) Connect USB cables between FPGA board and PC via micro-USB ports.
3) Turn on power switch for FPGA board.
4) Open Quartus Programmer to program FPGA through USB-1 by following step.
    i) Click “Hardware Setup…” to select
        - AGF FPGA Development Kit [USB-1] for Agilex F-series
        - USB-BlasterII [USB-1] for Arria10 SoC
    ii) Click “Auto Detect” and select FPGA number.
    iii) Select FPGA device icon (Agilex or A10SoC).
    iv) Click “Change File” button, select SOF file in pop-up window and click “open” button.
    v) Check “program”.
    vi) Click “Start” button to program FPGA.
    vii) Wait until Progress status is equal to 100%.

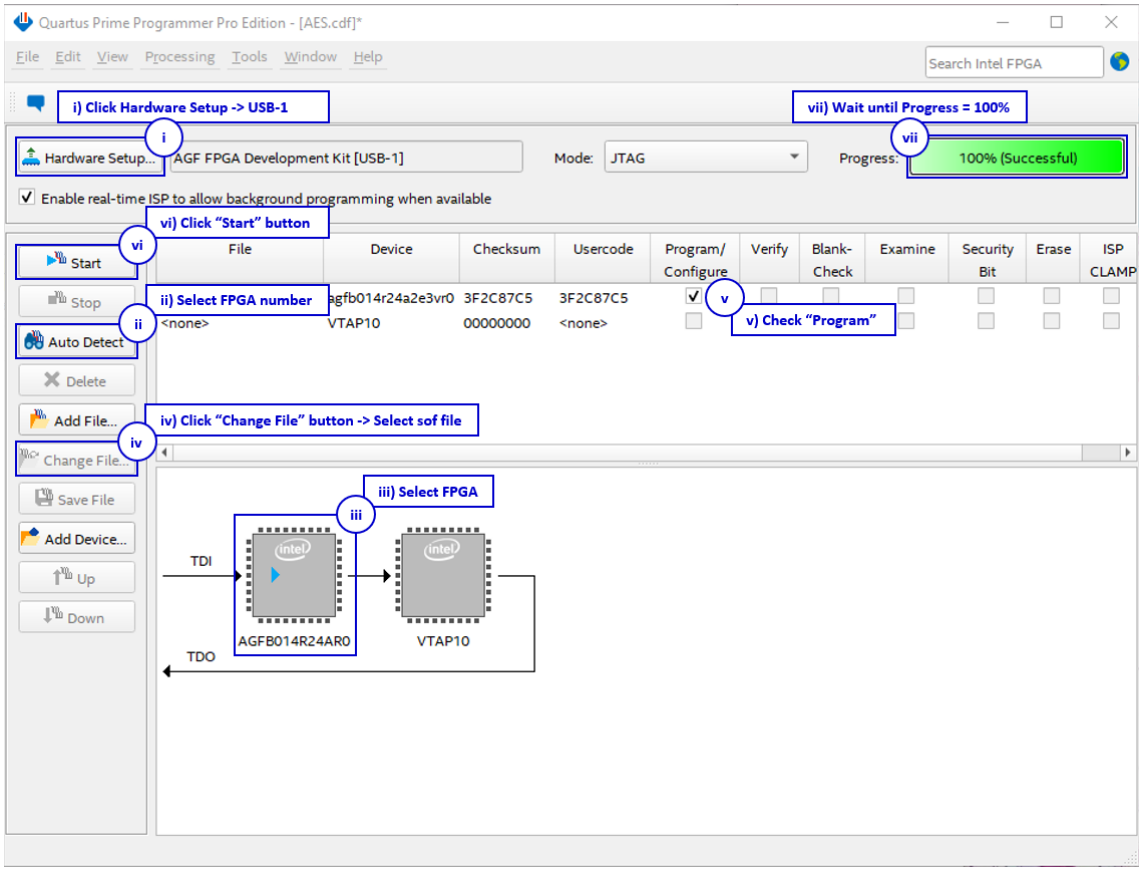

Figure 2-1 FPGA Programmer for Agilex

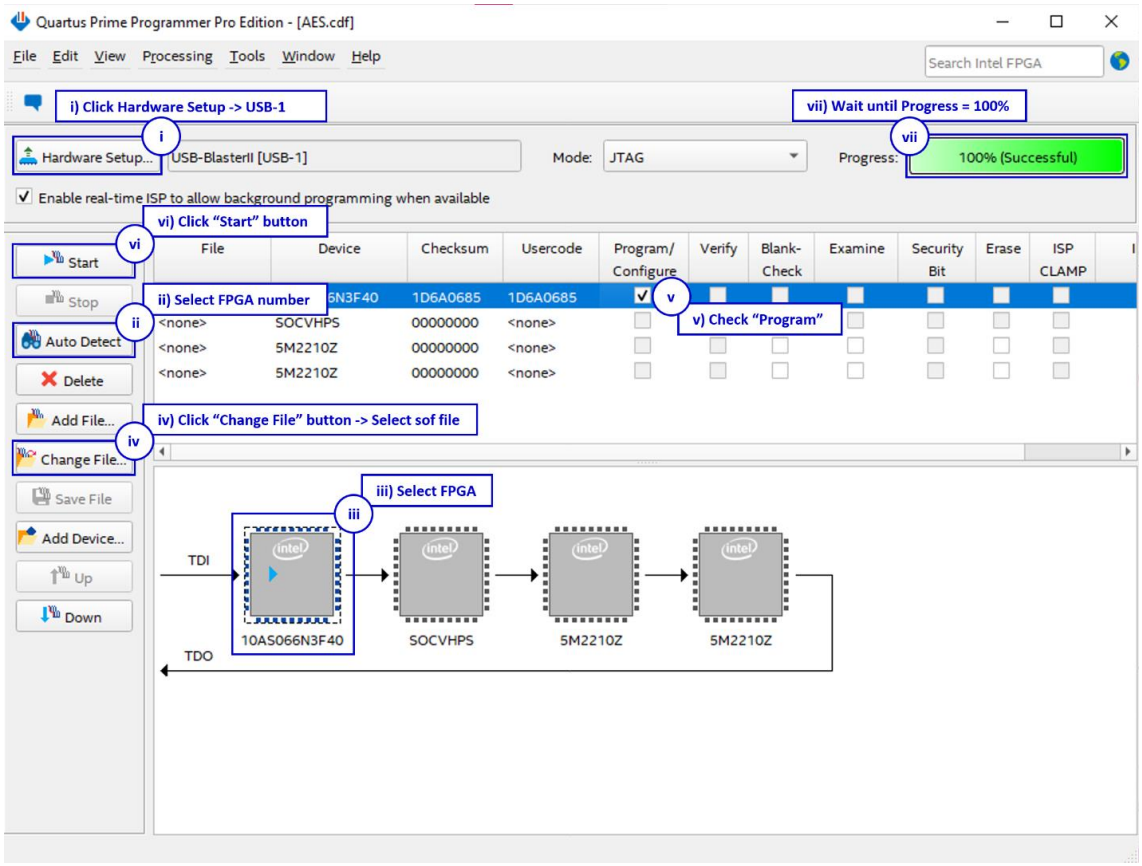

Figure 2-2 FPGA Programmer for A10SoC

For A10SoC after program SOF file complete, Quartus Prime will show popup message of Intel FPGA IP Evaluation Mode Status as shown in Figure 2-3. Please do not press cancel button.

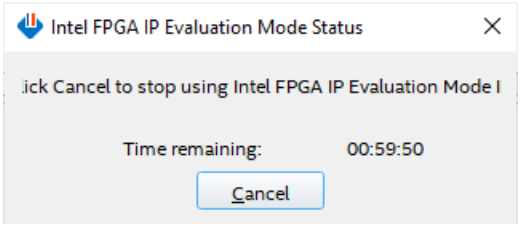

Figure 2-3 Intel FPGA IP Evaluation Mode Status

3 Nios II Command Shell

User can fill RAMs with plain or cipher data patterns, set encryption key, set tweakable key, IV and control test operation via Nios II Command Shell. When configuration is completed, AES256XTSdemo command menu will be displayed as shown in Figure 3-1. The detailed information of each menu is described in topic 4.

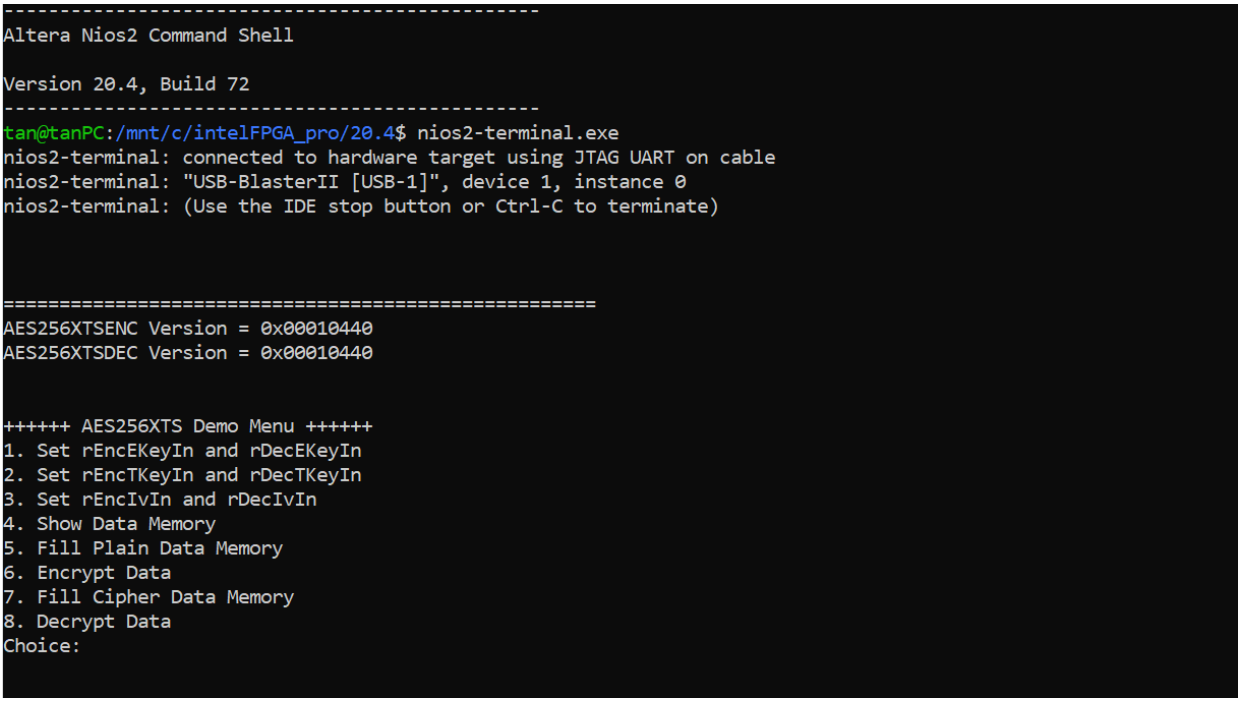

Figure 3-1 Nios II Command Shell

4 Command detail and testing result

4.1 Set encryption key

Step to set encryption key as follows

a) Select “1. Set rEncEKeyIn and rDecEKeyIn”.
b) Current rEncEKeyIn will be displayed on Nios II Command Shell as shown in Figure 4-1.
c) Set new rEncEKeyIn: 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 rDecEKeyIn key will be displayed on Nios II Command Shell.
e) Set new rDecEKeyIn key: User is allowed to input new key in hex format or press “enter” to use rEncEKeyIn as rDecEKeyIn. Then the current decryption key is printed again.

```
====================================================
AES256XTSENC Version = 0x00010440
AES256XTSDEC Version = 0x00010440


++++++ AES256XTS Demo Menu ++++++
1. Set rEncEKeyIn and rDecEKeyIn
2. Set rEncTKeyIn and rDecTKeyIn
3. Set rEncIvIn and rDecIvIn
4. Show Data Memory
5. Fill Plain Data Memory
6. Encrypt Data
7. Fill Cipher Data Memory
8. Decrypt Data
Choice: 1

+++ Set rEncEKeyIn and rDecEKeyIn +++
               rEncEKeyIn= 0x0000000000000000000000000000000000000000000000000000000000000000
(enter to use rEncEKeyIn)= 0x00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
          new rEncEKeyIn= 0x00112233445566778899AABBCCDDEEFF00112233445566778899AABBCCDDEEFF

               rDecEKeyIn= 0x0000000000000000000000000000000000000000000000000000000000000000
(enter to use rEncEKeyIn)= 0x
          new rDecEKeyIn= 0x00112233445566778899AABBCCDDEEFF00112233445566778899AABBCCDDEEFF
```

Figure 4-1 Set rEncEKeyIn and rDecEKeyIn example

4.2 Set tweakable key

Step to set tweakable key as follows

a) Select “2. Set rEncTKeyIn and rDecTKeyIn”.
b) Current rEncTKeyIn will be displayed on Nios II Command Shell as shown in Figure 4-2.
c) Set new rEncTKeyIn: 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 rDecTKeyIn will be displayed on Nios II Command Shell.
e) Set new rDecTKeyIn: User is allowed to input new key in hex format or press “enter” to use rEncTKeyIn as rDecTKeyIn. Then the current decryption key is printed again.

Figure 4-2 Set rEncTKeyIn and rDecTKeyIn example

4.3 Set encryption/decryption IV

Step to Set encryption/decryption IV as follows

a) Select “3. Set rEncIvIn and rDecIvIn”.
b) Current rEncIvIn will be displayed on Nios II Command Shell as shown in Figure 4-3.
c) Set new rEncIvIn: User is allowed to input new IV in hex format or press “enter” to skip setting new key. Then the current encryption IV is printed again.
d) Current rDecIvIn will be displayed on Nios II Command Shell.
e) Set new rDecIvIn: User is allowed to input new IV in hex format or press “enter” to use rEncIvIn as rDecIvIn. Then the current decryption IV is printed again.

```
++++++ AES256XTS Demo Menu ++++++
1. Set rEncEKeyIn and rDecEKeyIn
2. Set rEncTKeyIn and rDecTKeyIn
3. Set rEncIvIn and rDecIvIn
4. Show Data Memory
5. Fill Plain Data Memory
6. Encrypt Data
7. Fill Cipher Data Memory
8. Decrypt Data
Choice: 3

+++ Set rEncIvIn and rDecIvIn +++
               rEncIvIn= 0x00000000000000000000000000000000
(enter to use rEncIvIn)= 0x0123456789abcdef0123456789abcdef
          new rEncIvIn= 0x0123456789ABCDEF0123456789ABCDEF

               rDecIvIn= 0x00000000000000000000000000000000
(enter to use rEncIvIn)= 0x
          new rDecIvIn= 0x0123456789ABCDEF0123456789ABCDEF
```

Figure 4-3 Set rEncIvIn and rDecIvIn example

4.4 Show Data Memory

To show data in memory, user can select “4. Show Data Memory” and input the desired length of data in byte to show. Both plain data and cipher data will be displayed in table-form as shown in Figure 4-4. User can press “enter” key to skip putting the number of data, then Nios II Command Shell will display 64 bytes (default value) of plain data and cipher data at address 0x0000-0x003F in four rows of table.

```
++++++ AES256XTS Demo Menu ++++++
1. Set rEncEKeyIn and rDecEKeyIn
2. Set rEncTKeyIn and rDecTKeyIn
3. Set rEncIvIn and rDecIvIn
4. Show Data Memory
5. Fill Plain Data Memory
6. Encrypt Data
7. Fill Cipher Data Memory
8. Decrypt Data
Choice: 4

+++ Show Data Memory +++
Number of Data in byte (enter = 64):

                Plain Data                          Cipher Data
Addr#  .0.....3 .4.....7 .8.....B .C.....F  .0.....3 .4.....7 .8.....B .C.....F
0000:  00000000 00000000 00000000 00000000  00000000 00000000 00000000 00000000
0001:  00000000 00000000 00000000 00000000  00000000 00000000 00000000 00000000
0002:  00000000 00000000 00000000 00000000  00000000 00000000 00000000 00000000
0003:  00000000 00000000 00000000 00000000  00000000 00000000 00000000 00000000
```

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

4.5 Fill Plain Data Memory

Step to fill plain data in memory as follows

a) Select “5. Fill Plain Data Memory”.
b) Input the desired length of data in byte. User can press “enter” to encrypt 16 Byte plain data. user can select data pattern.
c) There are four pattern to fill memory.
    a. zero pattern
    b. 8-bit counter
    c. 16-bit counter
    d. 32-bit counter
d) Whole plain-data memory is filled with selected data pattern.

```
++++++ AES256XTS Demo Menu ++++++
1. Set rEncEKeyIn and rDecEKeyIn
2. Set rEncTKeyIn and rDecTKeyIn
3. Set rEncIvIn and rDecIvIn
4. Show Data Memory
5. Fill Plain Data Memory
6. Encrypt Data
7. Fill Cipher Data Memory
8. Decrypt Data
Choice: 5

+++ Fill Plain Data Memory +++
Length of Plain Data in byte (enter = 16): 40
a. zero pattern
b. 8-bit counter
c. 16-bit counter
d. 32-bit counter
Choice: b

Length of Plain Data : 40

                Plain Data                          Cipher Data
Addr#  .0.....3 .4.....7 .8.....B .C.....F  .0.....3 .4.....7 .8.....B .C.....F
0000:  00010203 04050607 08090A0B 0C0D0E0F  00000000 00000000 00000000 00000000
0001:  10111213 14151617 18191A1B 1C1D1E1F  00000000 00000000 00000000 00000000
0002:  20212223 24252627 00000000 00000000  00000000 00000000 00000000 00000000
```

Figure 4-5 Displayed Data when select pattern b

4.6 Encrypt

Select “6. Encrypt” to encrypt plain data in memory. When the encryption process is finished, both plain data and cipher data will be displayed in table-form as shown in Figure 4-6.

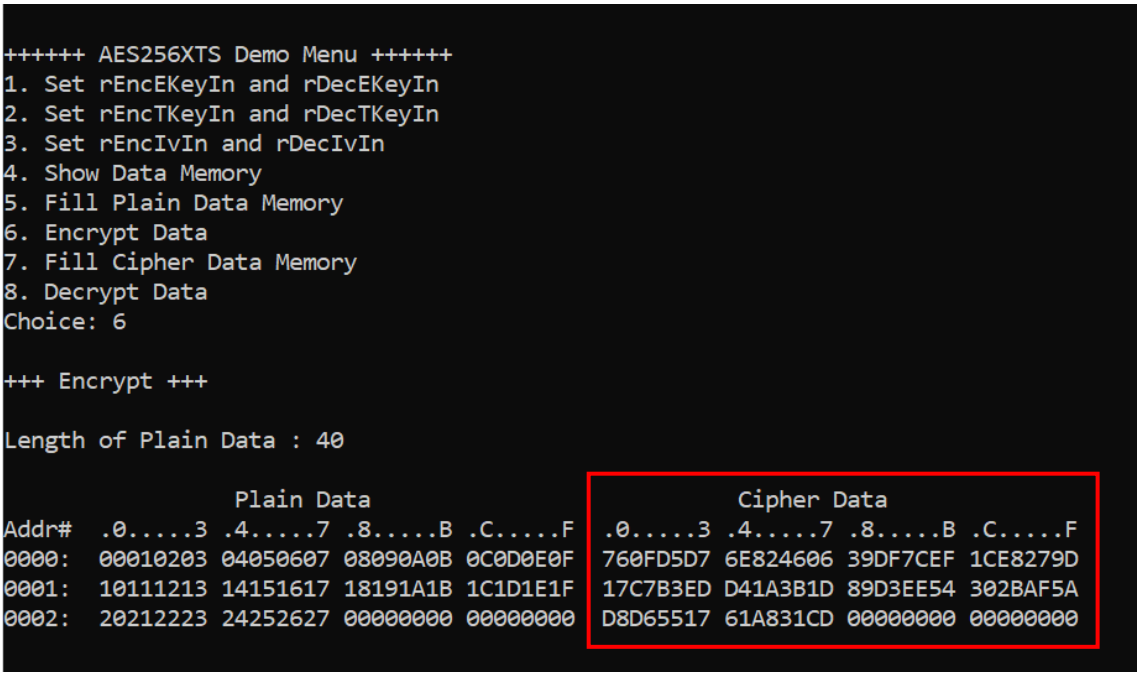

Figure 4-6 Nios II Command Shell after finished encryption process

4.7 Fill Cipher Data Memory

Step to fill Cipher data in memory as follows

a) Select “7. Fill Cipher Data Memory”.
b) Input the desired length of data in byte. User can press “enter” to decrypt 16 Byte Cipher data. user can select data pattern.
c) There are four pattern to fill memory.
    a. zero pattern
    b. 8-bit counter
    c. 16-bit counter
    d. 32-bit counter
d) Whole cipher-data memory is filled with selected data pattern.

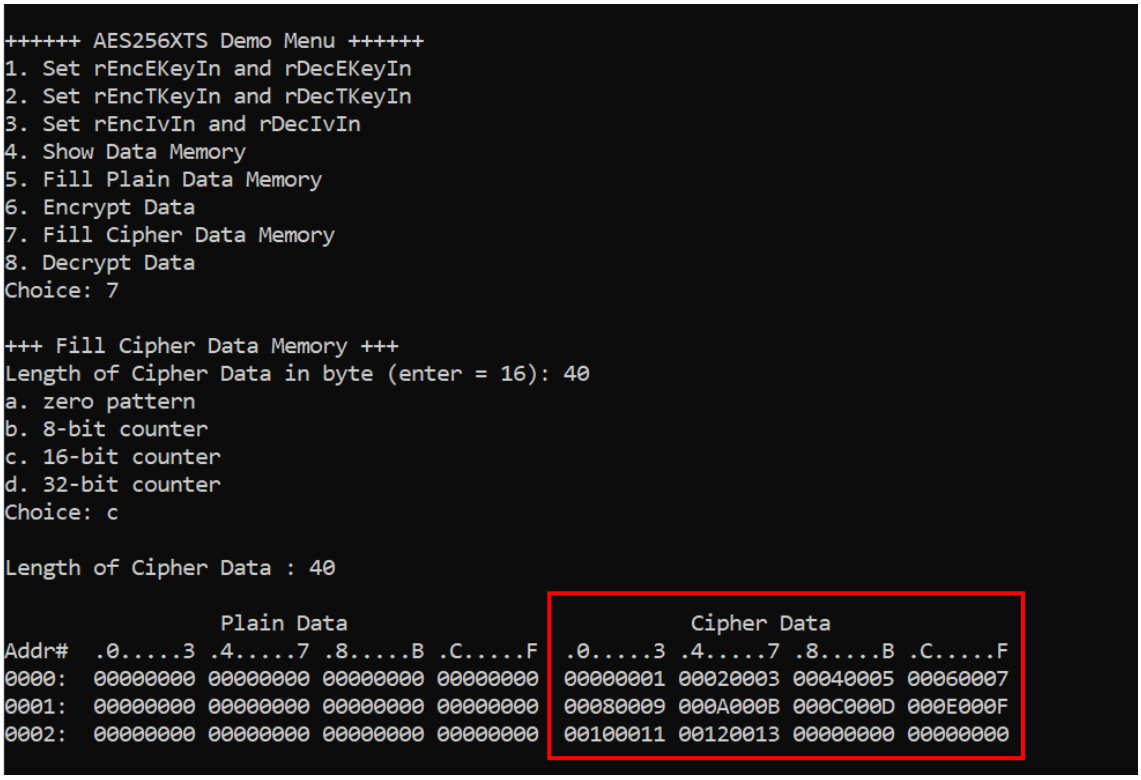

Figure 4-7 Displayed Data when select pattern c

4.8 Decrypt

Select “8. Decrypt Data” to decrypt cipher data in memory. When the decryption process is finished, both plain data and cipher data will be displayed in table-form as shown in Figure 4-8.

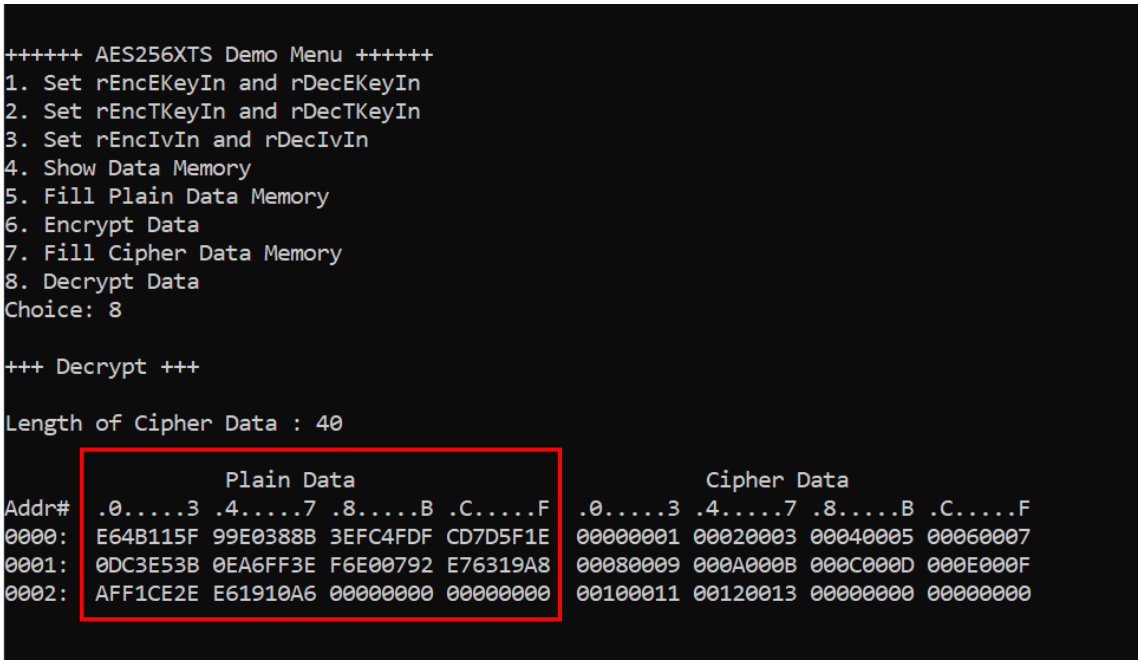

Figure 4-8 Nios II Command Shell after finished decryption process

5 Revision History

Revision	Date	Description
1.00	30-Nov-2022	Initial version release