嵌入式系統期末專題

組員：
林庭毅 S1052016 電機四
陳冠維 S1052020 電機四
羅豐祥 S1052025 電機四
陳祥鈞 S1023137 電機四

完整電路輸出

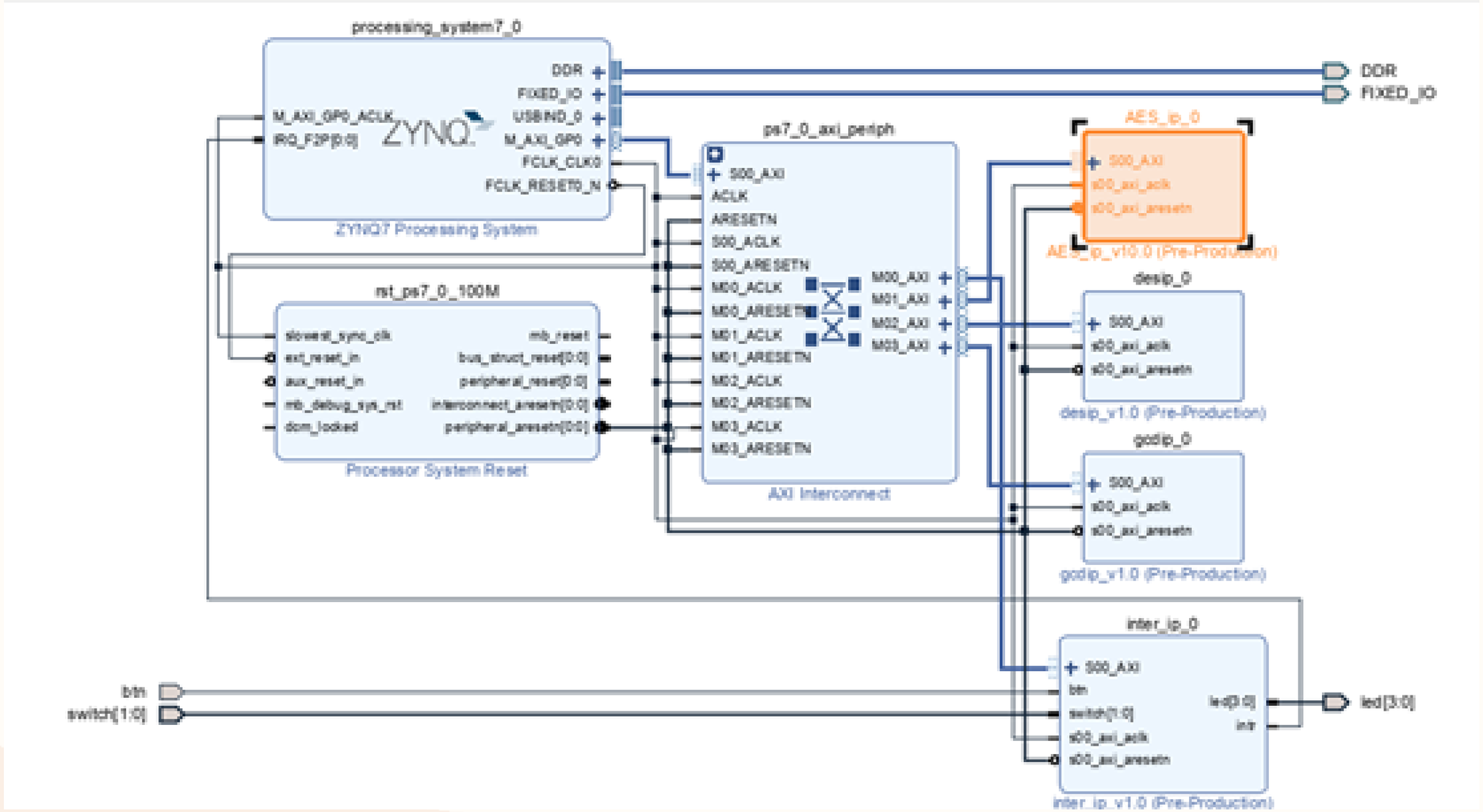


圖1 完整電路輸出

AES時序圖(加密成功)

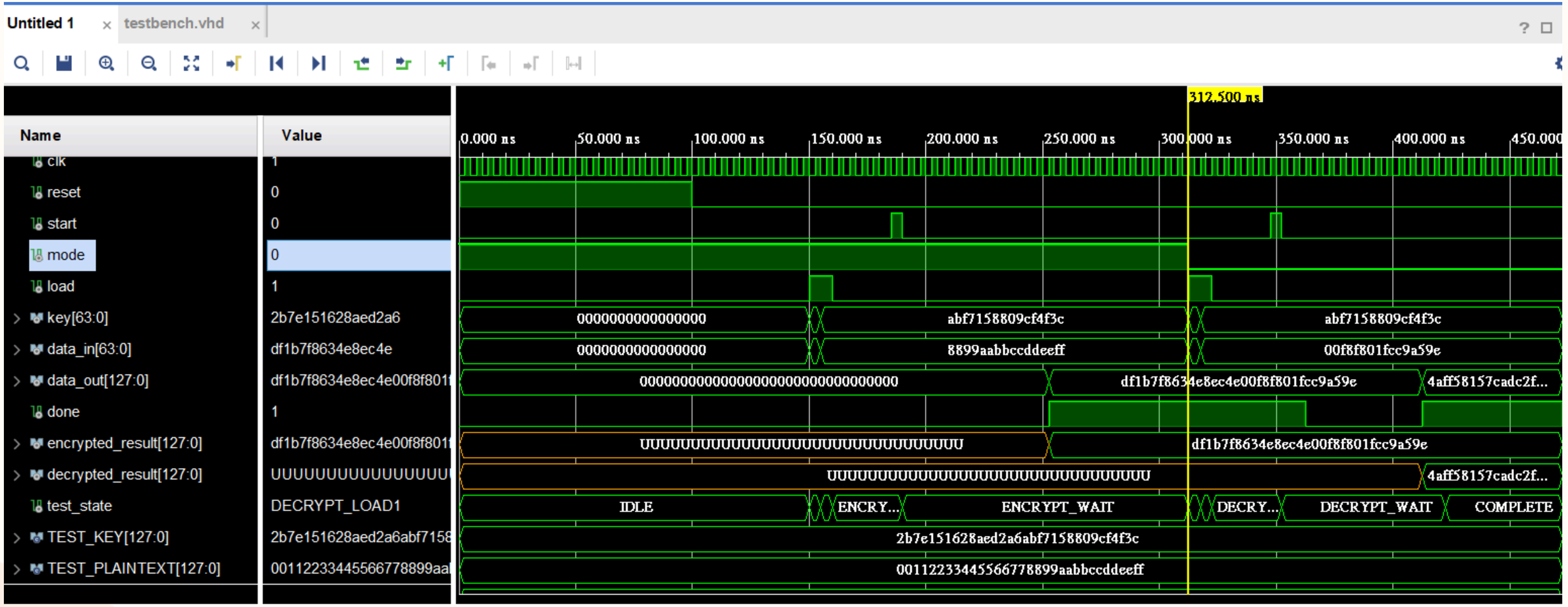
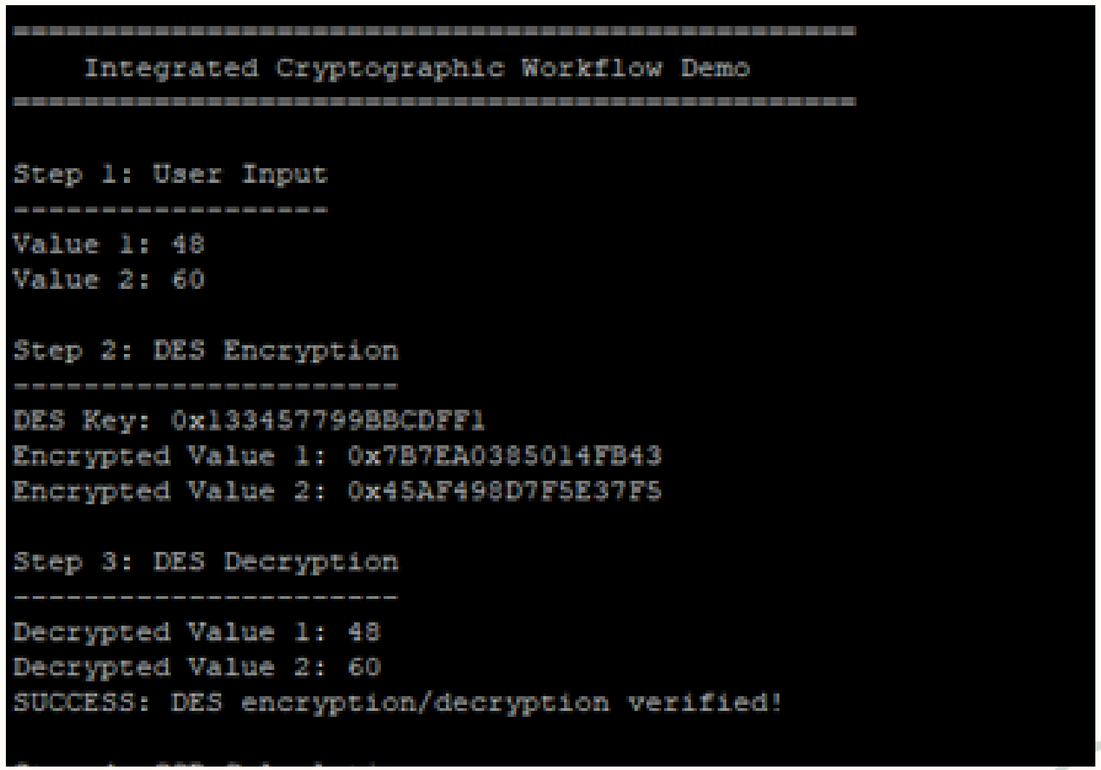


圖2 AES時序圖

Standalone

1。使用者輸入慾處理數據
2。DES 加解密
3。GCD 找出最大公因數
4。將最大公因數使用 AES 加密
5。LED 閃縮表示程序結束



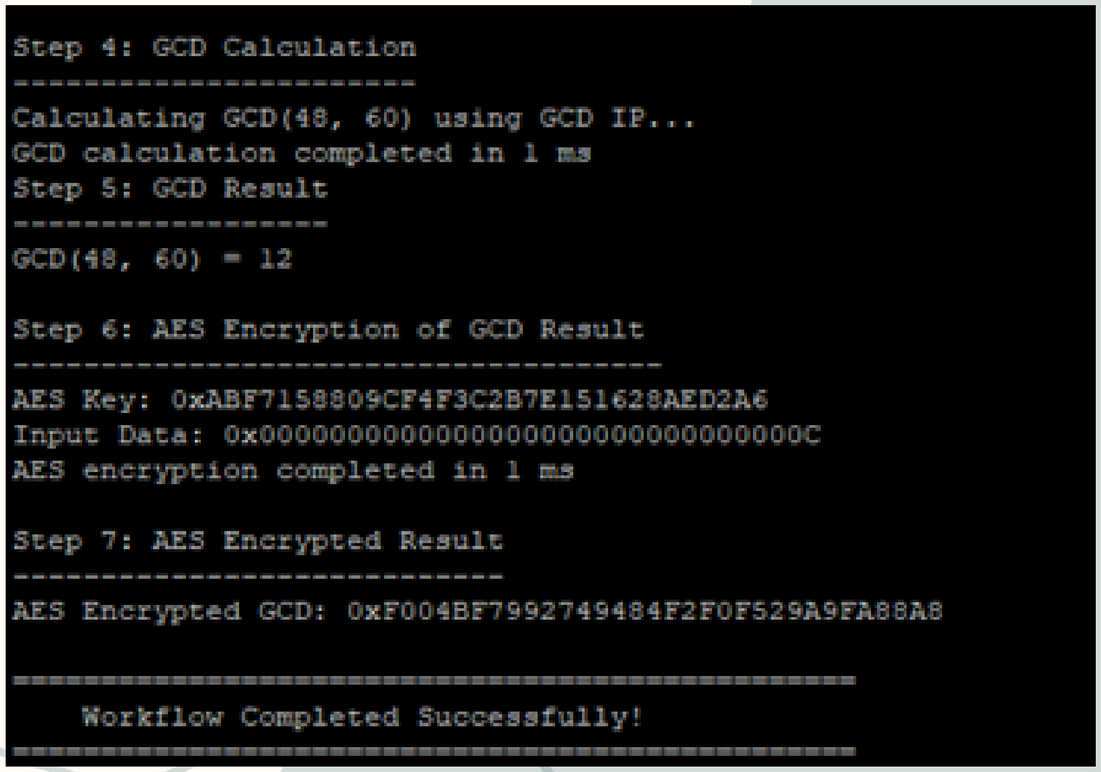


圖3 Putty 輸出端

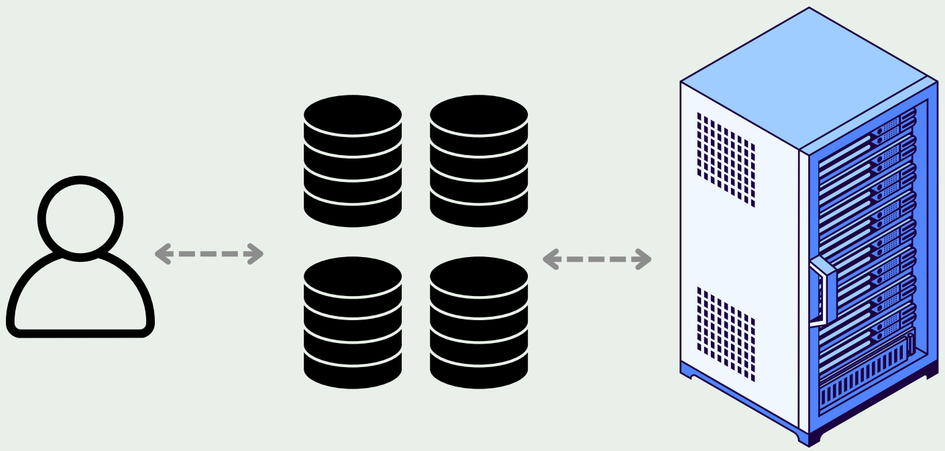
FreeRTOS

增加測試功能：

1。每四秒會多一個使用者輸入

2。輸入但尚未被處理的值，會在佇列等待

3。預設系統每次執行計算需要間格10秒



```
Encrypted value1: 0x2D95CA36844116B4
Encrypted value2: 0xCFDB52B7B81268DD
Data queued for processing

>>> USER INPUT <<<
User entered values: 84, 126
Encrypted value1: 0xD99E074773C8FBF3
Encrypted value2: 0x9D38F45C072E1069
Queue full! Data lost.

[STATUS] Queue items waiting: 2

>>> USER INPUT <<<
User entered values: 84, 126
Encrypted value1: 0xD99E074773C8FBF3
Encrypted value2: 0x9D38F45C072E1069
Queue full! Data lost.

=== SYSTEM PROCESSING CYCLE ===
Processing values: 100, 150

[STATUS] Queue items waiting: 1
Decrypted values: 100, 150
GCD(100, 150) = 50
AES encrypted GCD result: 0x2D35E8CF292107C9
Processing completed successfully!
```

```
>>> USER INPUT <<<
User entered values: 84, 126
Encrypted value1: 0xD99E074773C8FBF3
Encrypted value2: 0x9D38F45C072E1069
Data queued for processing

[STATUS] Queue items waiting: 2
>>> ALL TEST INPUTS COMPLETED <<<

=== SYSTEM PROCESSING CYCLE ===
Processing values: 17, 19

[STATUS] Queue items waiting: 1
Decrypted values: 17, 19
GCD(17, 19) = 1
AES encrypted GCD result: 0x1523A8FF47B1D916
Processing completed successfully!

[STATUS] Queue items waiting: 1

=== SYSTEM PROCESSING CYCLE ===
Processing values: 84, 126

[STATUS] Queue items waiting: 0
Decrypted values: 84, 126
GCD(84, 126) = 42
AES encrypted GCD result: 0xDBB365614C27ED6F
Processing completed successfully!

[STATUS] Queue items waiting: 0

=== SYSTEM PROCESSING CYCLE ===
No data in queue to process
All inputs processed. System processing will continue monitoring.
```

圖4 Free RTOS 執行結果

Interrupt

增加功能：

1。Switch 可提供功能模式切換

2。Push Button 提供模式確認及系統進程推進功能

模式選擇：

Auto Mode　　:自動運行

Manual Mode :手動選擇輸入且自行點擊Push Button 確認

Debug Mode　:顯示詳細資訊

Simple Mode　:使用最簡單的輸入進行測試

Input		Output		
SW0	SW1	Mode	Case	
			Value 1	Value 2
0	0	Auto Mode	12	8
0	1	Manual Mode	49	18
1	0	Debug Mode	144	96
1	1	Simple Mode	255	85

表一 Switch 輸入對應模式與 Input Case

Interrupt

```
================================================
Restarting system...
================================================

=== Stage 1: Mode Selection ===
Use 2 Switch combination to select operation mode:
SW1 SW0 = Mode
0   0   = Auto Mode (fully automatic execution)
0   1   = Manual Mode (pushbutton confirmation for each step)
1   0   = Debug Mode (show detailed intermediate results)
1   1   = Simple Mode (minimal output for quick testing)
Press pushbutton to confirm selection

Current selection: SW1=0 SW0=0 = Mode 0 - Auto Mode
Current selection: SW1=0 SW0=1 = Mode 1 - Manual Mode
Mode confirmed: 1

=== Stage 2: Test Case Selection ===
=== Value Input Instructions ===
Use 2 Switch combination to select test case:
SW1 SW0 = Test Case
0   0   = Case 0: Values 12, 8   (simple case)
0   1   = Case 1: Values 48, 18  (medium case)
1   0   = Case 2: Values 144, 96 (complex case)
1   1   = Case 3: Values 255, 85 (max complexity)

Press pushbutton when ready
Test case confirmed: 1
```

```
Test case 1 selected: Value1=48, Value2=18

=== Starting Cryptographic Workflow ===
Processing values: 48 and 18

=== Stage 3: DES Encryption ===
DES encryption completed
Encrypted Value 1: 0x7B7EA0385014FB43
Encrypted Value 2: 0x81a47DF4D287CF53
Press pushbutton to continue...

=== Stage 4: DES Decryption Verification ===
DES verification SUCCESS: decrypted values 48, 18
Decrypted Value 1: 0x0000000000000030
Decrypted Value 2: 0x0000000000000012
Press pushbutton to continue...

=== Stage 5: GCD Calculation ===
GCD(48, 18) = 6
Press pushbutton to continue...

=== Stage 6: AES Encryption of GCD Result ===
AES Encrypted Result: 0xE4FB886BC8F045C37D72F5E55BAF4B9C

=== Stage 7: Workflow Complete ===
All cryptographic operations completed!

Press pushbutton to restart...
Press pushbutton to continue...

================================================
Restarting system...
================================================
```

圖5 Manual Mode

Linux Driver

增加功能：

1。顯示模組載入資訊及硬體輸入資訊

2。腳位及功能自動測試

IP名稱	Device Tree節點
inter_ip_0	inter_ip@43c00000
AES_ip_0	aes_ip@43c10000
desip_0	des_ip@43c20000
gcdip_0	gcd_ip@43c30000

表二 IP對應Device Tree節點

Linux Driver

```
root@pynqz2:~# insmod crypto_ips.ko
major: 243
virtual irq: 48
Crypto IPs module loaded successfully
INTER: 0x43c00000 => 71aaf2f8
AES: 0x43c10000 => d3c4bb24
DES: 0x43c20000 => 5e5bd9e6
GCD: 0x43c30000 => e1a4e547
root@pynqz2:~# lsmod
Module                  Size  Used by
crypto_ips             16384  0
char2platform          16384  0
uio_pdrv_genirq        16384  0
root@pynqz2:~# ./switch_read
```

```
root@pynqz2:~# ./switch_read
SWITCH data (read): 0
SWITCH data (ioctl): 0
root@pynqz2:~# ./led_control ll
LED pattern set to: ll (0xB)
root@pynqz2:~# ./crypto_test
```

圖6 模組載入資訊、switch按鈕值、寫入led燈值

Linux Driver

```
root@pynqz2:~# ./crypto_test
================================================
    Crypto IPs Individual Test Program
================================================

=== Switch/LED Test ===
Current switch value: 0
Testing LED patterns...
Setting LED pattern: 0x1
Setting LED pattern: 0x3
Setting LED pattern: 0x6
Setting LED pattern: 0x9
Setting LED pattern: 0xC
Setting LED pattern: 0xF
Setting LED pattern: 0xA
Switch/LED Test: COMPLETED

=== DES Test ===
Key: 0x0000000000418C1C
Plaintext: 0x0000000000418C2C
Encrypted: 0x0000000000418C5C
Decrypted: 0x0000000000418C8C
DES Test: PASSED
```

```
=== GCD Test ===
GCD(48, 18) = 6
GCD(144, 96) = 48
GCD Test: COMPLETED

=== AES Test ===
Key: 0x09CF4F3CABF7158828AED2A62B7E1516
Input: 0x7393172AE93D7E112E409F966BC1BEE2
Output: 0xDF761F6541A3422FDD4D6791B8D37244
AES Test: COMPLETED

All tests completed!
root@pynqz2:~#
```

圖7 腳位以及功能測試

Linux Driver

```
/include/ "system-conf.dtsi"
/ {

        amba {
                /* AES IP  */
                aes_ip: aes_ip@43c10000 {
                        compatible = "xlnx,aes-ip-1.00";
                        reg = <0x43c10000 0x1000>;
                        xlnx,s00-axi-data-width = <32>;
                        xlnx,s00-axi-addr-width = <6>;
                };

                /* DES IP  */
                des_ip: des_ip@43c20000 {
                        compatible = "xlnx,des-ip-1.00";
                        reg = <0x43c20000 0x1000>;
                        xlnx,s00-axi-data-width = <32>;
                        xlnx,s00-axi-addr-width = <6>;
                };
```

```
                /* GCD IP  */
                gcd_ip: gcd_ip@43c30000 {
                        compatible = "xlnx,gcd-ip-1.00";
                        reg = <0x43c30000 0x1000>;
                        xlnx,s00-axi-data-width = <32>;
                        xlnx,s00-axi-addr-width = <6>;
                };

                /* INTER IP */
                inter_ip: inter_ip@43c00000 {
                        compatible = "xlnx,myhwip-1.00";
                        interrupt-parent = <&intc>;
                        interrupts = <0 29 1>;
                        reg = <0x43c00000 0x1000>;
                        xlnx,s00-axi-data-width = <32>;
                        xlnx,s00-axi-addr-width = <6>;
                };
        };

        usb_phy0: phy0 {
                compatible = "ulpi-phy";
                #phy-cells = <0>;
```

圖8 system-conf.dtsi編譯前修改