Test Vector Generation for Block Ciphers

The user must prepare test vectors before running data acquisition. User defined scripts or scripts provided with FOBOS can be used.
The dataAcquisition.py script will send the test vectors one at a time and collect traces from the oscilloscope.
The blockCipherTVGen.py can be used to generate test vectors to be used by block ciphers. The script is located at fobos/sources

Here is a brief description for the test vector format

Supported commands

```
00C0 # pdi fifo (length in bytes to follow)
00C1 # sdi fifo (length in bytes to follow)
00C2 # rdi fifo (length in bytes to follow)
0081 # store expected output size (expected output size in bytes to follow)
0080 # select command register (command to follow)
```

FOBOS Protocol Example

Here is an example of a signle test vector of the FOBOS protocol format:

```
00C0 # pdi fifo (length in bytes to follow); FOBOS_CONTROL must assert di_valid
0008 # 8 bytes
FFFF
FFFF
FFFF
FFFF # 8 bytes, 16 bits at a time
00C1 # sdi fifo (length in bytes to follow)
000A # 10 bytes
0000
0000
0000
0000
0000 # 10 bytes, 16 bits at a time
0081 # store expected output size
0008 # 8 bytes of output expected
0080 # select command register
0001 # "start signal"
```

Using the script

The blockCipherTVGen.py is located at fobos/sources.
There are two steps to use it:

1- Set user defined parameters.
2- Run the script. It will generate the test vector file and plaintext file (not required for acquisition).

User Defined Parameters

```
############user defined settings
TRACE_NUM = <>              #Number of traces (plaintexts blocks to be sent to DUT) e.g 1000
PDI_LENGTH = <>             #Plaintext length in byets e.g 16
SDI_LENGTH = <>             #Key length in bytes e.g. 16
EXPECTED_OUT = <>           #Expected output in bytes i.e ciphertext length e.g 16
DIN_FILE = <>               #desitination file name e.g dinFile.txt
FIXED_KEY = <>              #Fixed key = yes | no e.g 'no'
KEY =  <>                   # Fixed key (if needed) e.g. '00112233445566778899AABBCCDDEEFF'
```

Example

Here is an example to generate 4 test vectors with 16 byte blocks, key and ciphertext. Key is fixed in this case:

```
############user defined settings
TRACE_NUM = 4           #Number of traces
PDI_LENGTH = 16         #In byets
SDI_LENGTH = 16          #In bytes
EXPECTED_OUT = 16          #expected output in bytes
DIN_FILE = 'dinFile.txt'  #desitination file name
FIXED_KEY = 'yes'        #Fixed key = yes | no
KEY =  '00112233445566778899AABBCCDDEEFF' # Fixed key (if needed)
```

```
$ python blockCipherTVGen.py
```

Here is how the generated dinFile.txt looks like.

```
$ cat dinFile.txt
00C00010B4900D0ECC646D4858C9125B3B61F76700C1001000112233445566778899AABBCCDDEEFF0081001000800001
00C00010E1361496BA8F078ED02DC1283C2F98C200C1001000112233445566778899AABBCCDDEEFF0081001000800001
00C0001050424A6E6EEED8C15D7DB737771FBE7400C1001000112233445566778899AABBCCDDEEFF0081001000800001
00C00010FCC8863498CD255ED57F864FD02824A800C1001000112233445566778899AABBCCDDEEFF0081001000800001
```

This file can now be used in FOBOS as a test vector file.