*****************Draft*****************
Crypto-Socket
Using AraratSnyapse Library
06/0720
*****************Draft*****************

A connection from RaspBian to Ultibo System "telnet 192.168.1.245 5050".

To isolate the variables I added the following record

```
GCM = record
  SockData:AnsiString;
  EncryptionTagToDecrypt:AnsiString;
  {EncryptionTag1 during teststr 1 or teststr 3 encrypt}
  EncryptionTag1:AnsiString;
  {EncryptionTag2 during teststr 1 or teststr 3 decrypt}
  EncryptionTag2:AnsiString;
  EncryptionTag3:AnsiString;
  PlainStr:AnsiString;
  CryptStr1:AnsiString;
  BinCryptStr1:AnsiString;
  cryptstr: AnsiString;
  tagstr: AnsiString;
  teststr: AnsiString;
  {Must be 16, 24 or 32 bytes}
  MyKey: AnsiString ;
  MyIV: AnsiString;
  MyAAD: AnsiString;
  MyData: AnsiString;
end;
```

The crypted string of bytes from the encryption plus the string of bytes from the Tag needs to be sent to the decrypt process.
The decryption is dependent on the Tag.

```
telnet 192.168.1.245 5050
Trying 192.168.1.245...
Connected to 192.168.1.245.
Escape character is '^]'.

112345678901234567890123456789012:My Secret IV:My Extra Secret AAD:The quick brown
testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz
```

This is what get written to the file test0605encrypt.txt

```
encrypt
112345678901234567890123456789012:My Secret IV:My Extra Secret AAD:The quick brown
testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz

GCM1.PlainStr
The quick brown testing a longer string not dependent on length 15 1234567890
abcdefghijklmnopqrstuvwxyz
```

```
GCM1.EncryptionTag1
f56c32e2ea3343b31748823b65590a09
GCM1.EncryptionTag2
f56c32e2ea3343b31748823b65590a09
GCM1.MyKey
12345678901234567890123456789012
GCM1.MyIV
My Secret IV
GCM1.MyAAD
My Extra Secret AAD
Decrypted
The quick brown testing a longer string not dependent on length 15 1234567890
abcdefghijklmnopqrstuvwxyz
EncryptionTag
f56c32e2ea3343b31748823b65590a09
Bytes Crypt
0e599f59da22536d4fe2d6bd48c118e594d7ee54ba178f1c918dfd69dea863b7514a8a263a5e5846b1
5de04945412b3f6334f78109d079d0f8198199c7a2ca297f376f1f97d1e3e75473538b943a6824b01c
ae711e8c1fedf0837660b99efc554ca60904d613420c
```

```
telnet 192.168.1.245 5050
Trying 192.168.1.245...
Connected to 192.168.1.245.
Escape character is '^]'.

212345678901234567890123456789012:My Secret IV:My Extra Secret
AAD:0e599f59da22536d4fe2d6bd48c118e594d7ee54ba178f1c918dfd69dea863b7514a8a263a5e5
846b15de04945412b3f6334f78109d079d0f8198199c7a2ca297f376f1f97d1e3e75473538b943a682
4b01cae711e8c1fedf0837660b99efc554ca60904d613420c:f56c32e2ea3343b31748823b65590a09
```

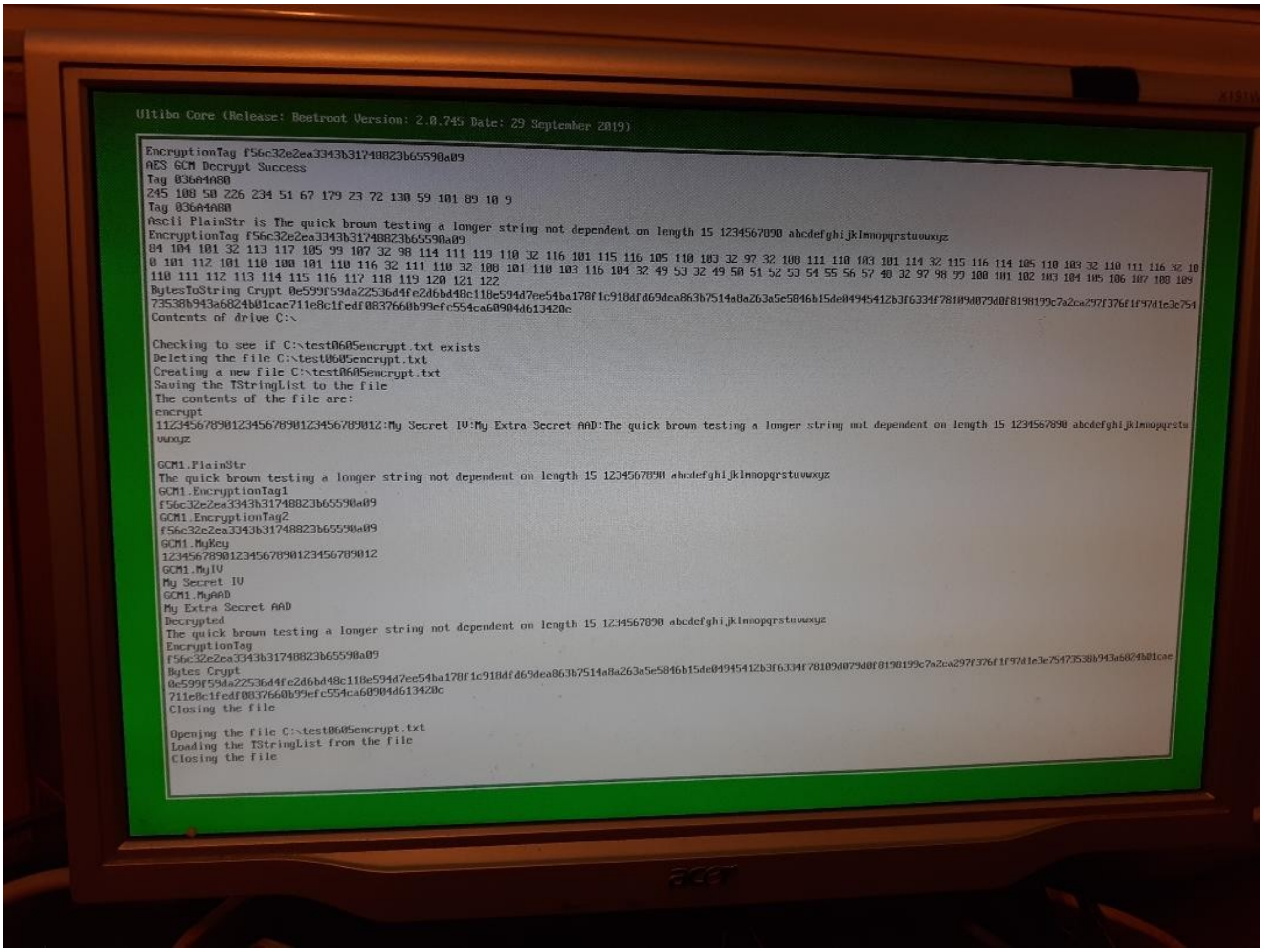
This is what get written to the file test0605decrypt.txt

```
decrypt
212345678901234567890123456789012:My Secret IV:My Extra Secret
AAD:0e599f59da22536d4fe2d6bd48c118e594d7ee54ba178f1c918dfd69dea863b7514a8a263a5e5
846b15de04945412b3f6334f78109d079d0f8198199c7a2ca297f376f1f97d1e3e75473538b943a682
4b01cae711e8c1fedf0837660b99efc554ca60904d613420c:f56c32e2ea3343b31748823b65590a09

GCM2.tagstr
f56c32e2ea3343b31748823b65590a09

GCM2.PlainStr
The quick brown testing a longer string not dependent on length 15 1234567890
abcdefghijklmnopqrstuvwxyz
GCM2.EncryptionTag2
f56c32e2ea3343b31748823b65590a09
GCM2.MyKey
12345678901234567890123456789012
GCM2.MyIV
My Secret IV
GCM2.MyAAD
My Extra Secret AAD
```

```
GCM2.EncryptionTagToDecrypt
f56c32e2ea3343b31748823b65590a09
MyKey
12345678901234567890123456789012
MyIV
My Secret IV
MyAAD
My Extra Secret AAD
Decrypted

EncryptionTag
f56c32e2ea3343b31748823b65590a09
EncryptionTagToDecrypt
f56c32e2ea3343b31748823b65590a09
```

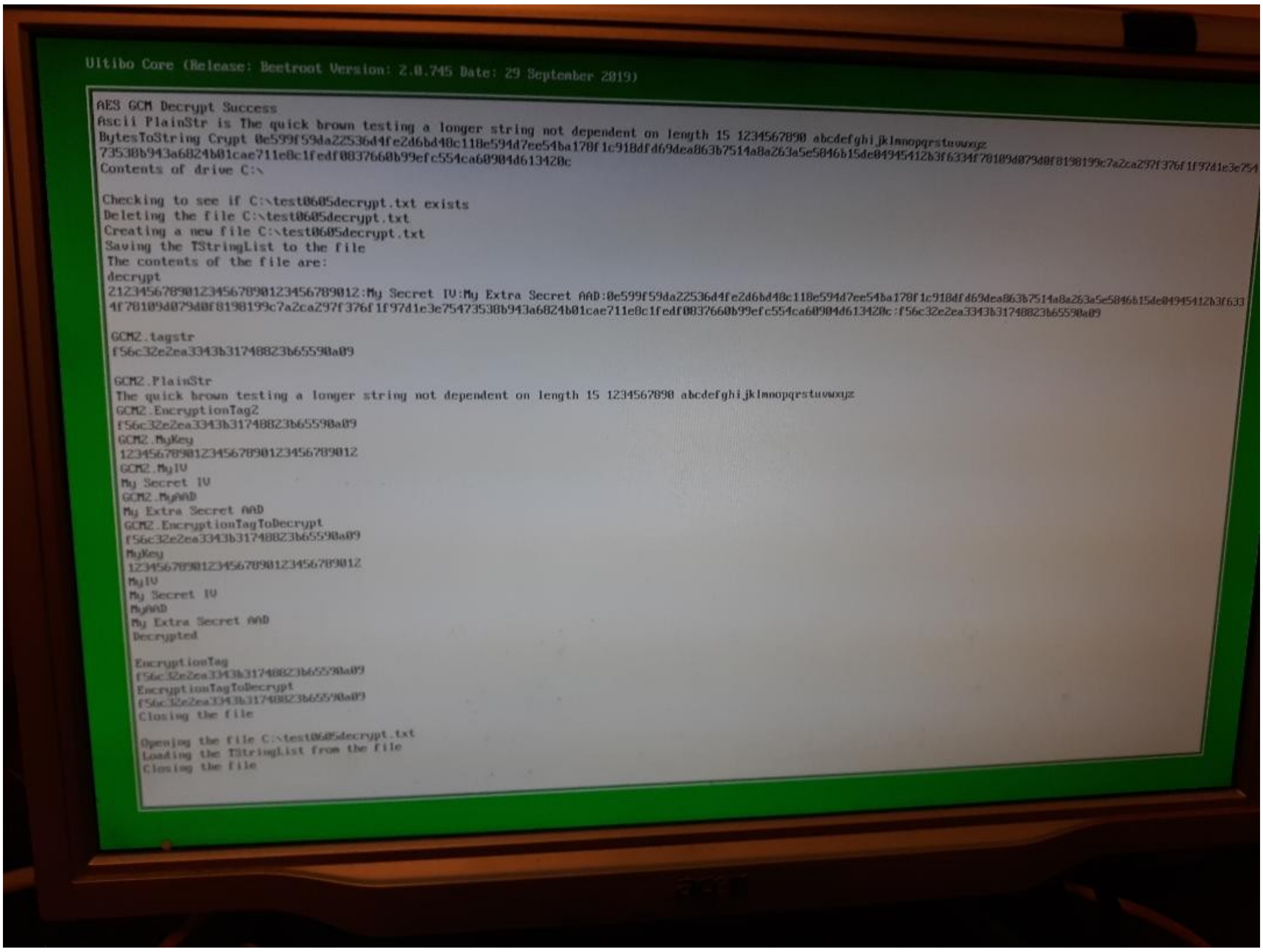
```
tftp 192.168.1.245
tftp> binary
tftp> get test0605encrypt.txt
Received 908 bytes in 0.0 seconds
tftp> get test0605decrypt.txt
Received 922 bytes in 0.0 seconds
tftp> quit
```

256 Bit encrypt



```
Ultibo Core (Release: Beetroot Version: 2.0.745 Date: 29 September 2019)

EncryptionTag f56c32e2ea3343b31748823b65590a09
AES GCM Decrypt Success
Tag 036A4A80
245 108 50 226 234 51 67 179 23 72 130 59 101 89 10 9
Tag 036A4A80
Ascii PlainStr is The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz
EncryptionTag f56c32e2ea3343b31748823b65590a09
84 104 101 32 113 117 105 99 107 32 98 114 111 119 110 32 116 101 115 116 105 110 103 32 97 32 108 111 110 103 101 114 32 115 116 114 105 110 103 32 110 111 116 32 10
0 101 112 101 110 100 101 110 116 32 111 110 32 108 101 110 103 116 104 32 49 53 32 49 50 51 52 53 54 55 56 57 48 32 97 98 99 100 101 102 103 104 105 106 107 108 109
110 111 112 113 114 115 116 117 118 119 120 121 122
BytesToString Crypt 0e599f59da22536d4fe2d6bd48c118e594d7ee54ba178f1c918dfd69dea863b7514a8a263a5e5846b15de04945412b3f6334f78109d079d0f8198199c7a2ca297f376f1f97d1e3c754
73538b943a6824b01cae711e8c1fedf0837660b99efc554ca60904d613420c
Contents of drive C:\

Checking to see if C:\test0605encrypt.txt exists
Deleting the file C:\test0605encrypt.txt
Creating a new file C:\test0605encrypt.txt
Saving the TStringList to the file
The contents of the file are:
encrypt
112345678901234567890123456789012:My Secret IV:My Extra Secret AAD:The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstu
vwxyz

GCM1.PlainStr
The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz
GCM1.EncryptionTag1
f56c32e2ea3343b31748823b65590a09
GCM1.EncryptionTag2
f56c32e2ea3343b31748823b65590a09
GCM1.MyKey
12345678901234567890123456789012
GCM1.MyIV
My Secret IV
GCM1.MyAAD
My Extra Secret AAD
Decrypted
The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz
EncryptionTag
f56c32e2ea3343b31748823b65590a09
Bytes Crypt
0e599f59da22536d4fe2d6bd48c118e594d7ee54ba178f1c918dfd69dea863b7514a8a263a5e5846b15de04945412b3f6334f78109d079d0f8198199c7a2ca297f376f1f97d1e3e75473538b943a6824b01cae
711e8c1fedf0837660b99efc554ca60904d613420c
Closing the file

Opening the file C:\test0605encrypt.txt
Loading the TStringList from the file
Closing the file
```

256 Bit decrypt



```
Ultibo Core (Release: Beetroot Version: 2.0.745 Date: 29 September 2019)

AES GCM Decrypt Success
Ascii PlainStr is The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz
BytesToString Crypt 0e599f59da22536d4fe2d6bd48c118e594d7ee54ba178f1c918dfd69dea863b7514a8a263a5e5846b15de04945412b3f6334f78109d079d0f8198199c7a2ca297f376f1f97d1e3e754
73538b943a6824b01cae711e8c1fedf0837660b99efc554ca60904d613420c
Contents of drive C:\

Checking to see if C:\test0605decrypt.txt exists
Deleting the file C:\test0605decrypt.txt
Creating a new file C:\test0605decrypt.txt
Saving the TStringList to the file
The contents of the file are:
decrypt
21234567890123456789012345678901 2:My Secret IV:My Extra Secret AAD:0e599f59da22536d4fe2d6bd48c118e594d7ee54ba178f1c918dfd69dea863b7514a8a263a5e5846b15de04945412b3f633
4f78109d079d0f8198199c7a2ca297f376f1f97d1e3e75473538b943a6824b01cae711e8c1fedf0837660b99efc554ca60904d613420c:f56c32e2ea3343b31748823b65590a09

GCM2.tagstr
f56c32e2ea3343b31748823b65590a09

GCM2.PlainStr
The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz
GCM2.EncryptionTag2
f56c32e2ea3343b31748823b65590a09
GCM2.MyKey
12345678901234567890123456789012
GCM2.MyIV
My Secret IV
GCM2.MyAAD
My Extra Secret AAD
GCM2.EncryptionTagToDecrypt
f56c32e2ea3343b31748823b65590a09
MyKey
12345678901234567890123456789012
MyIV
My Secret IV
MyAAD
My Extra Secret AAD
Decrypted

EncryptionTag
f56c32e2ea3343b31748823b65590a09
EncryptionTagToDecrypt
f56c32e2ea3343b31748823b65590a09
Closing the file

Opening the file C:\test0605decrypt.txt
Loading the TStringList from the file
Closing the file
```

Background: Started with 2 projects test_crypto.lpi & Srv.lpi from github devlone Ultibo_Projects.

Commad line using FPC

Step 1
. ~/fpc.sh

Step 2
cd Ultibo_Projects/Crypto-Socket/Rpi3/ or cd Ultibo_Projects/Crypto-Socket/RPi2/

Step 3
compile

```
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI3B -Fu../../../AraratSynapse
@/home/devel/ultibo/core/fpc/bin/RPI3.CFG -O2 Srv.lpr
```

or

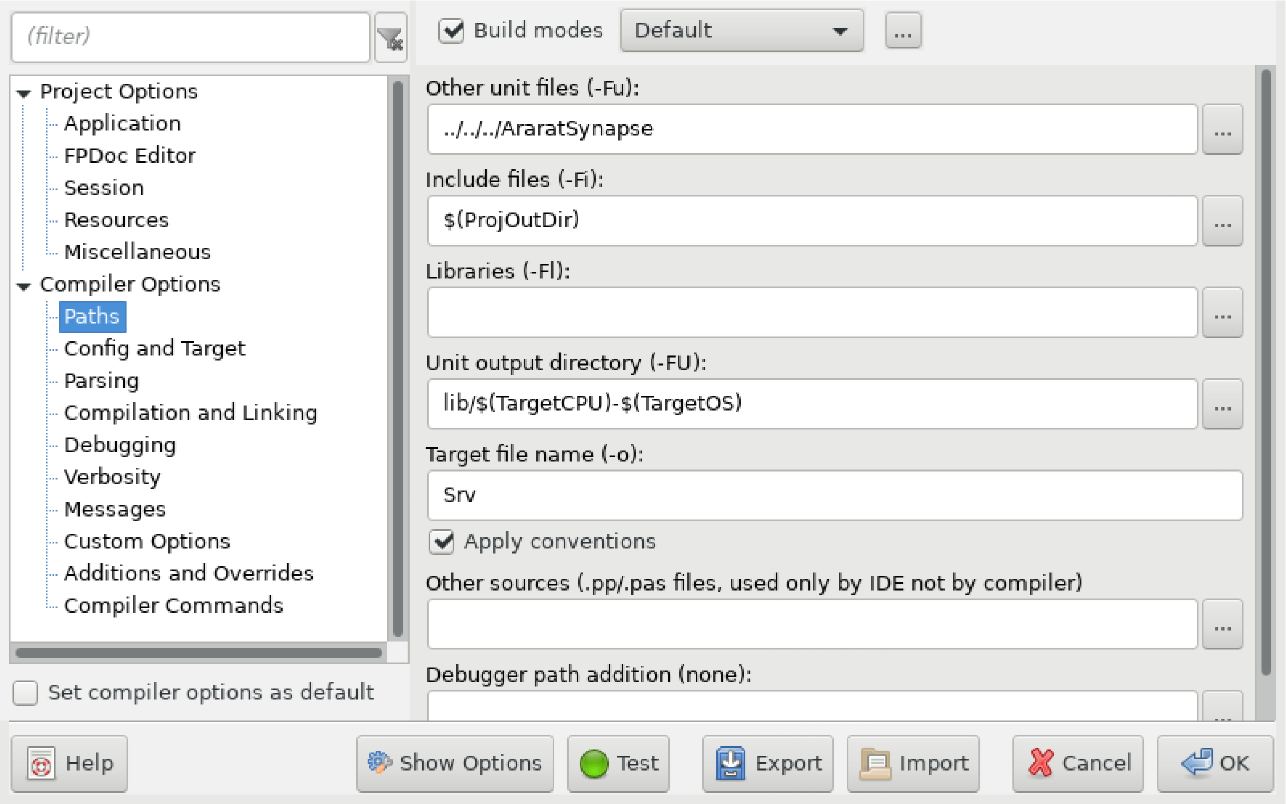
```
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI2B -Fu../../../AraratSynapse
@/home/devel/ultibo/core/fpc/bin/RPI2.CFG -O2 Srv.lpr
```

Transfer kernel7.img

```
./upker7.sh
```

```
Updating kernel7.img
tftp> tftp> Sent 2718380 bytes in 10.7 seconds
tftp> done
```

Compiling with Lazaraus.



☑ Build modes: Default

Other unit files (-Fu): ../../../AraratSynapse

Include files (-Fi): $(ProjOutDir)

Libraries (-Fl):

Unit output directory (-FU): lib/$(TargetCPU)-$(TargetOS)

Target file name (-o): Srv

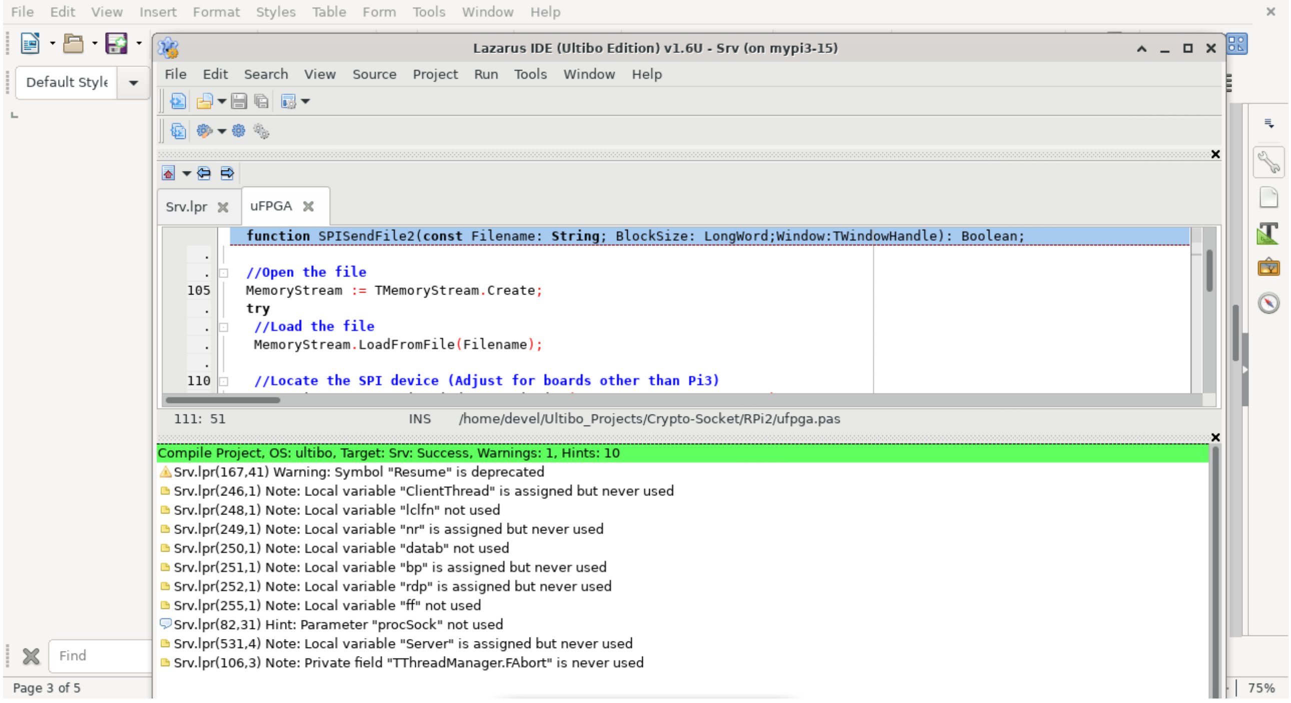
☑ Apply conventions

Other sources (.pp/.pas files, used only by IDE not by compiler)

Debugger path addition (none):

□ Set compiler options as default

Depress Run/Compile



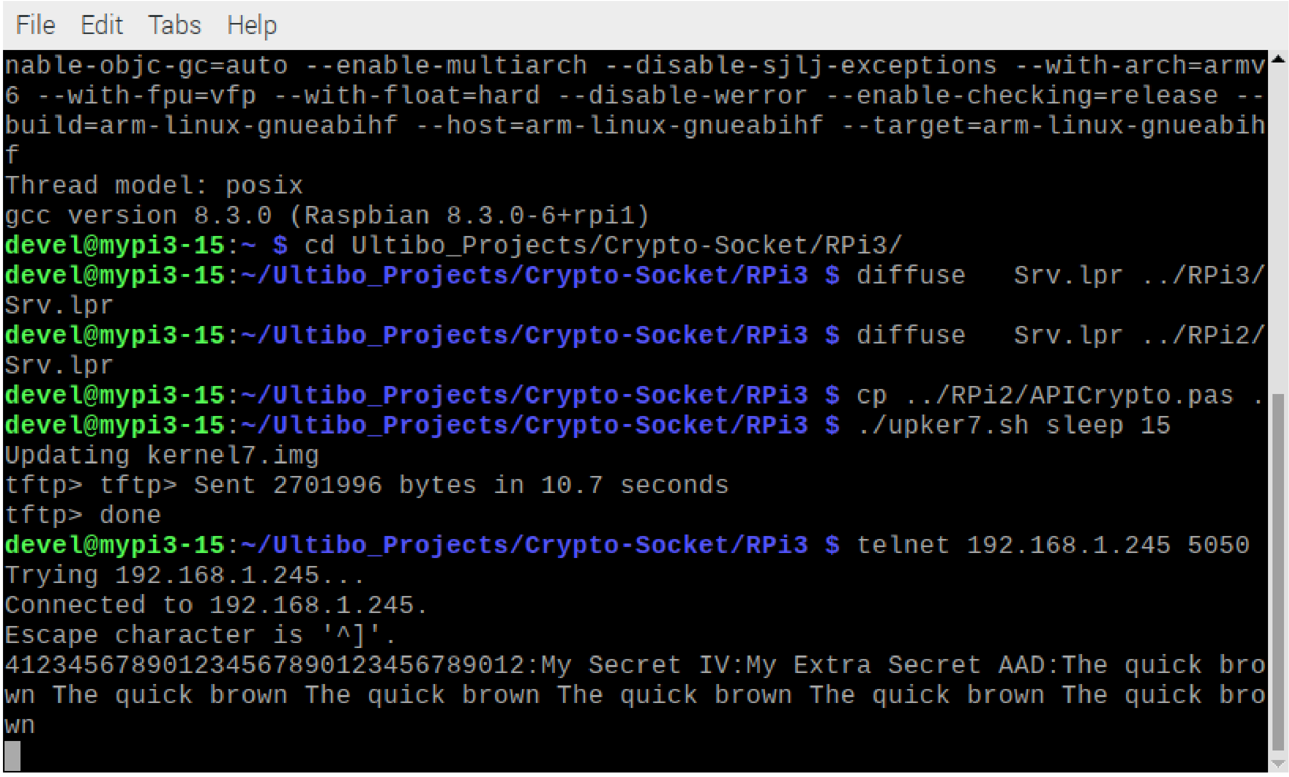
File Edit View Insert Format Styles Table Form Tools Window Help
Default Style
Lazarus IDE (Ultibo Edition) v1.6U - Srv (on mypi3-15)
File Edit Search View Source Project Run Tools Window Help
Srv.lpr
uFPGA
Find
Page 3 of 5
75%

```
function SPISendFile2(const Filename: String; BlockSize: LongWord;Window:TWindowHandle): Boolean;

//Open the file
MemoryStream := TMemoryStream.Create;
try
 //Load the file
 MemoryStream.LoadFromFile(Filename);

 //Locate the SPI device (Adjust for boards other than Pi3)
```

```
111: 51          INS     /home/devel/Ultibo_Projects/Crypto-Socket/RPi2/ufpga.pas
```

```
Compile Project, OS: ultibo, Target: Srv: Success, Warnings: 1, Hints: 10
Srv.lpr(167,41) Warning: Symbol "Resume" is deprecated
Srv.lpr(246,1) Note: Local variable "ClientThread" is assigned but never used
Srv.lpr(248,1) Note: Local variable "lclfn" not used
Srv.lpr(249,1) Note: Local variable "nr" is assigned but never used
Srv.lpr(250,1) Note: Local variable "datab" not used
Srv.lpr(251,1) Note: Local variable "bp" is assigned but never used
Srv.lpr(252,1) Note: Local variable "rdp" is assigned but never used
Srv.lpr(255,1) Note: Local variable "ff" not used
Srv.lpr(82,31) Hint: Parameter "procSock" not used
Srv.lpr(531,4) Note: Local variable "Server" is assigned but never used
Srv.lpr(106,3) Note: Private field "TThreadManager.FAbort" is never used
```

Telnet



```
nable-objc-gc=auto --enable-multiarch --disable-sjlj-exceptions --with-arch=armv
6 --with-fpu=vfp --with-float=hard --disable-werror --enable-checking=release --
build=arm-linux-gnueabihf --host=arm-linux-gnueabihf --target=arm-linux-gnueabih
f
Thread model: posix
gcc version 8.3.0 (Raspbian 8.3.0-6+rpi1)
devel@mypi3-15:~ $ cd Ultibo_Projects/Crypto-Socket/RPi3/
devel@mypi3-15:~/Ultibo_Projects/Crypto-Socket/RPi3 $ diffuse   Srv.lpr ../RPi3/
Srv.lpr
devel@mypi3-15:~/Ultibo_Projects/Crypto-Socket/RPi3 $ diffuse   Srv.lpr ../RPi2/
Srv.lpr
devel@mypi3-15:~/Ultibo_Projects/Crypto-Socket/RPi3 $ cp ../RPi2/APICrypto.pas .
devel@mypi3-15:~/Ultibo_Projects/Crypto-Socket/RPi3 $ ./upker7.sh sleep 15
Updating kernel7.img
tftp> tftp> Sent 2701996 bytes in 10.7 seconds
tftp> done
devel@mypi3-15:~/Ultibo_Projects/Crypto-Socket/RPi3 $ telnet 192.168.1.245 5050
Trying 192.168.1.245...
Connected to 192.168.1.245.
Escape character is '^]'.
412345678901234567890123456789012:My Secret IV:My Extra Secret AAD:The quick bro
wn The quick brown The quick brown The quick brown The quick brown The quick bro
wn
```