**********Draft**********

Crypto-Socket
Using AraratSnyapse Library
05/29/20

**********Draft**********

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

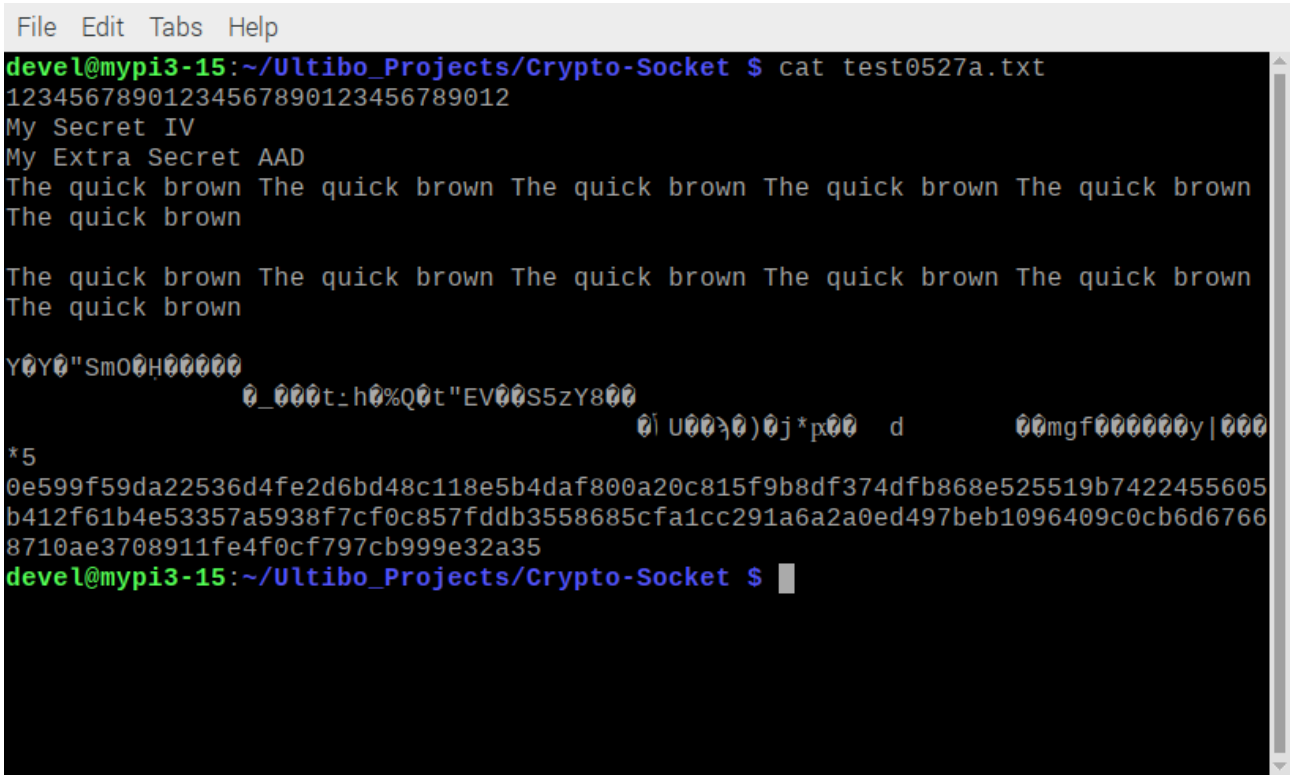
The initial values were below.
MyKey: AnsiString = '1234567890123456'; {Must be 16, 24 or 32 bytes}
MyIV: AnsiString = 'My Secret IV';
MyAAD: AnsiString = 'My Extra Secret AAD';
MyData: AnsiString = 'The quick brown fox jumps over the lazy dog.The quick brown fox jumps over the lazy dog.';

when the string below is sent to the Ultibo System

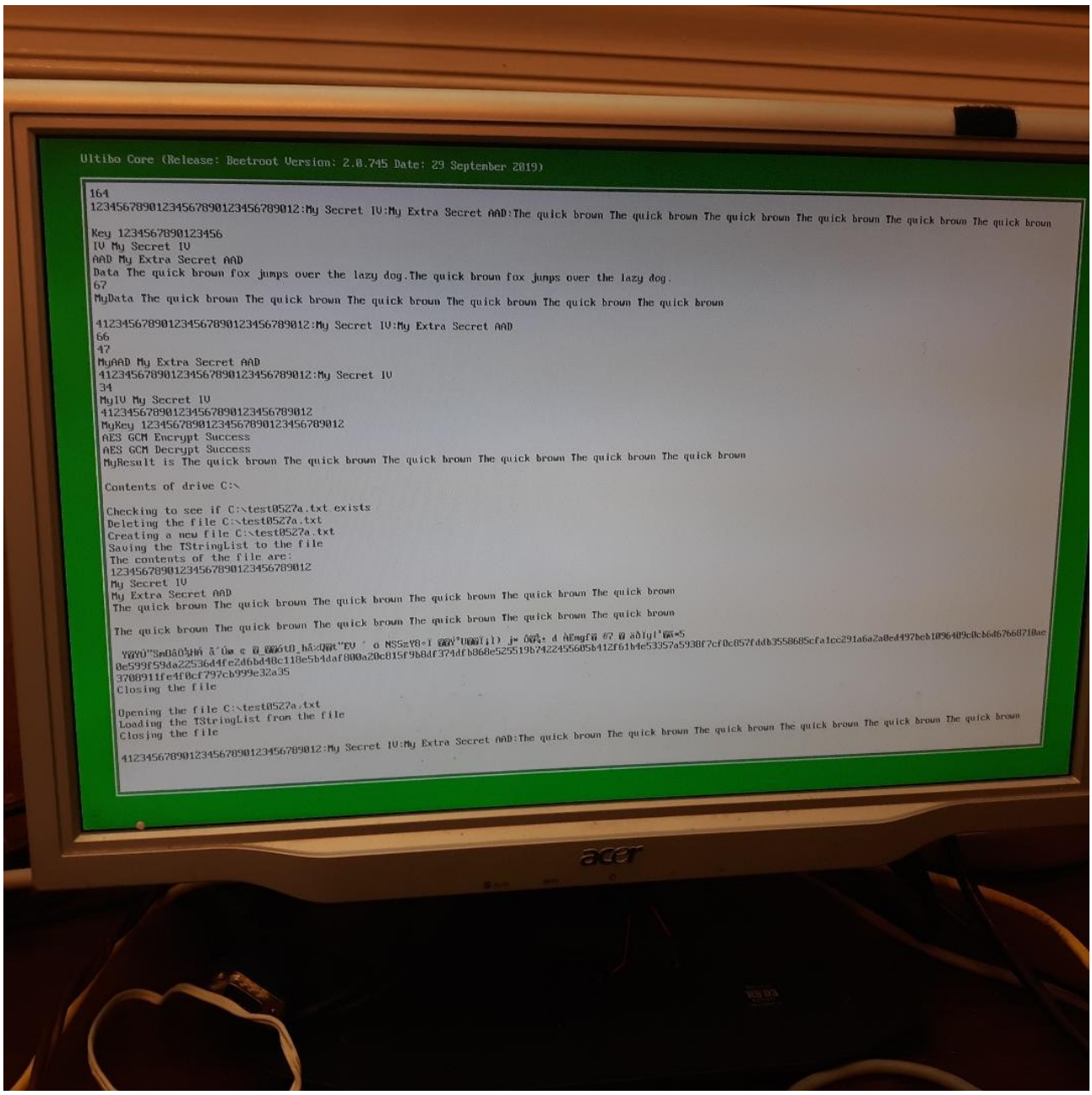
41234567890123456789012345678901 2:My Secret IV:My Extra Secret AAD:The quick brown The quick brown The quick brown The quick brown The quick brown The quick brown
The delimiter is :
MyKey 12345678901234567890123456789012
MyIV My Secret IV
MyAAD My Extra Secret AAD
MyData The quick brown The quick brown The quick brown The quick brown The quick brown The quick brown The quick brown

The results are writen to file test0527.txt

tftp 192.168.1.245
tftp> binary
tftp> get test0527.txt
Received 366 bytes in 0.0 seconds
tftp> quit


File Edit Tabs Help
devel@mypi3-15:~/Ultibo_Projects/Crypto-Socket $ cat test0527a.txt
12345678901234567890123456789012
My Secret IV
My Extra Secret AAD
The quick brown The quick brown The quick brown The quick brown The quick brown
The quick brown
The quick brown The quick brown The quick brown The quick brown The quick brown
The quick brown
Y@Y@"SmO@H@@@@@
@_@@@t:h@%Q@t"EV@@S5zY8@@
@i U@@\@@)@j*p@@ d @@mgf@@@@@@y|@@@
*5
0e599f59da22536d4fe2d6bd48c118e5b4daf800a20c815f9b8df374dfb868e525519b7422455605
b412f61b4e53357a5938f7cf0c857fddb3558685cfa1cc291a6a2a0ed497beb1096409c0cb6d6766
8710ae3708911fe4f0cf797cb999e32a35
devel@mypi3-15:~/Ultibo_Projects/Crypto-Socket $

256Bit Key



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

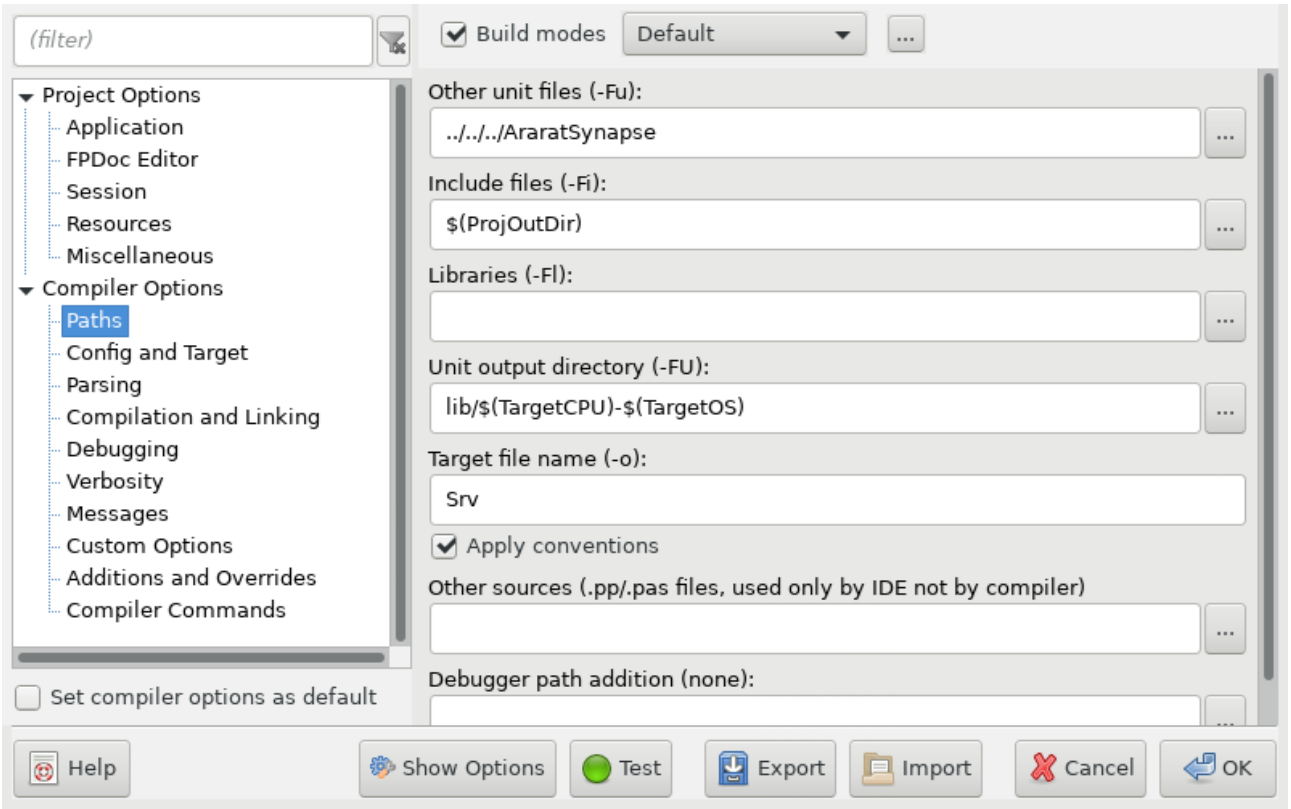
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI3B -Fu../../../AraratSynapse
@/home/devel/ultibo/core/fpc/bin/RPI3.CFG -O2 Srv.lpr

or

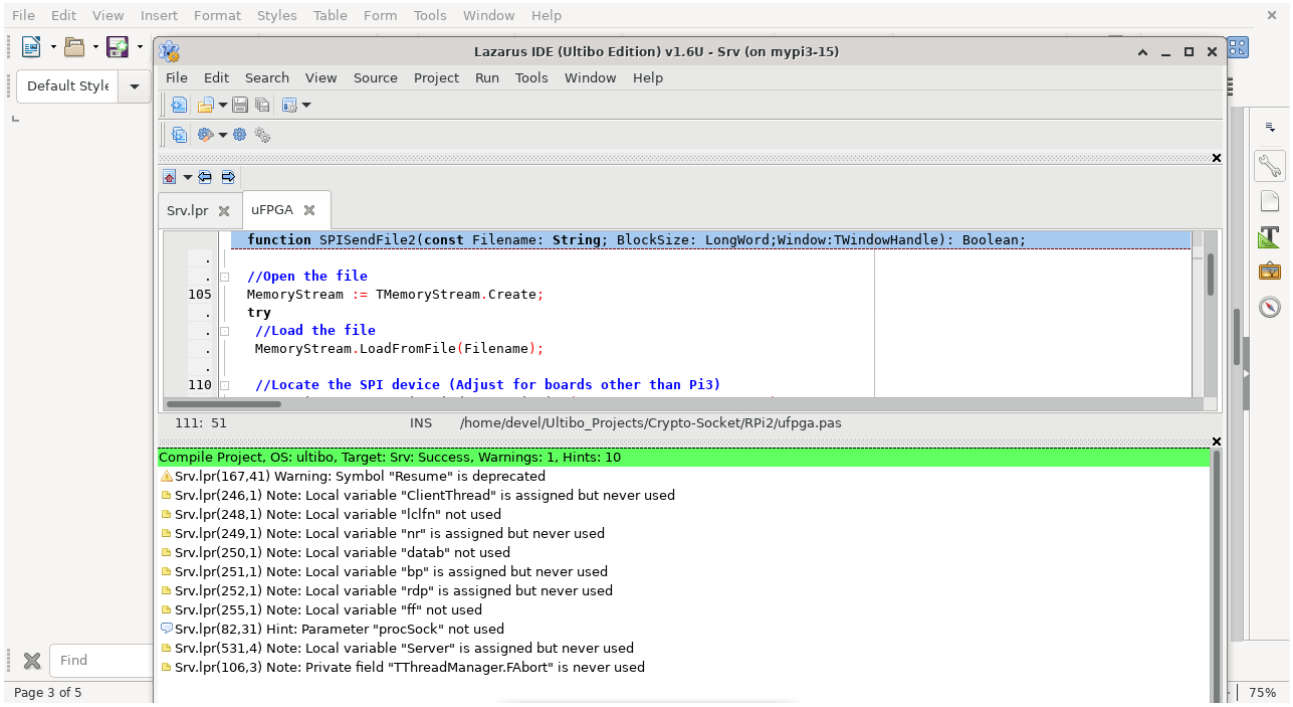
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI2B -Fu../../../AraratSynapse
@/home/devel/ultibo/core/fpc/bin/RPI2.CFG -O2 Srv.lpr
Transfer kernel7.img

To transfer kernel7.img
tftp 192.168.1.69 < cmdstftp
tftp> tftp> Sent 2701996 bytes in 5.3 seconds

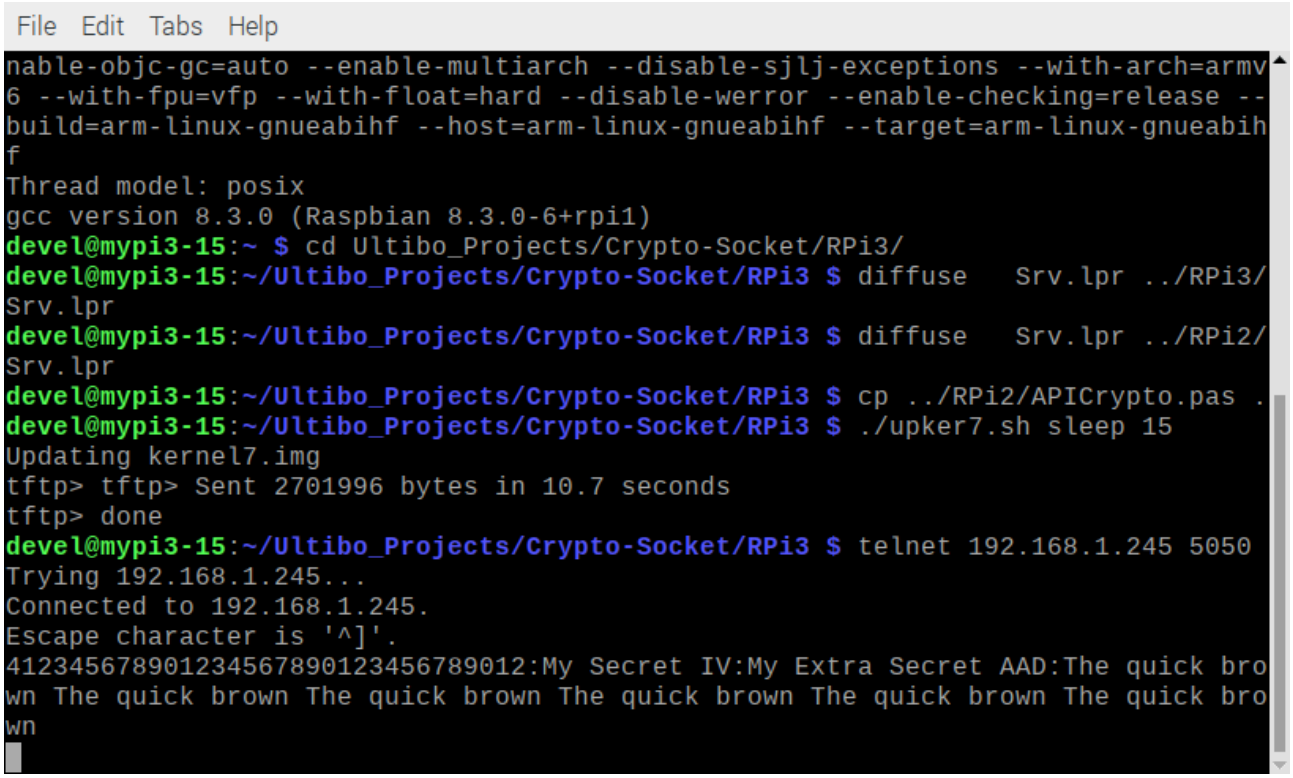
Compiling with Lazaraus.



Depress Run/Compile


Lazarus IDE (Ultibo Edition) v1.6U - Srv (on mypi3-15)
File Edit Search View Source Project Run Tools Window Help
Srv.lpr
uFPGA
function SPISendFile2(const Filename: String; BlockSize: LongWord;Window:TWindowHandle): Boolean;
//Open the file
105 MemoryStream := TMemoryStream.Create;
try
//Load the file
MemoryStream.LoadFromFile(Filename);
110 //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


File Edit Tabs Help
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 '^]'.
41234567890123456789012345678901 2: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