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

Crypto-Socket
Using AraratSnyapse Library
06/05/20

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

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

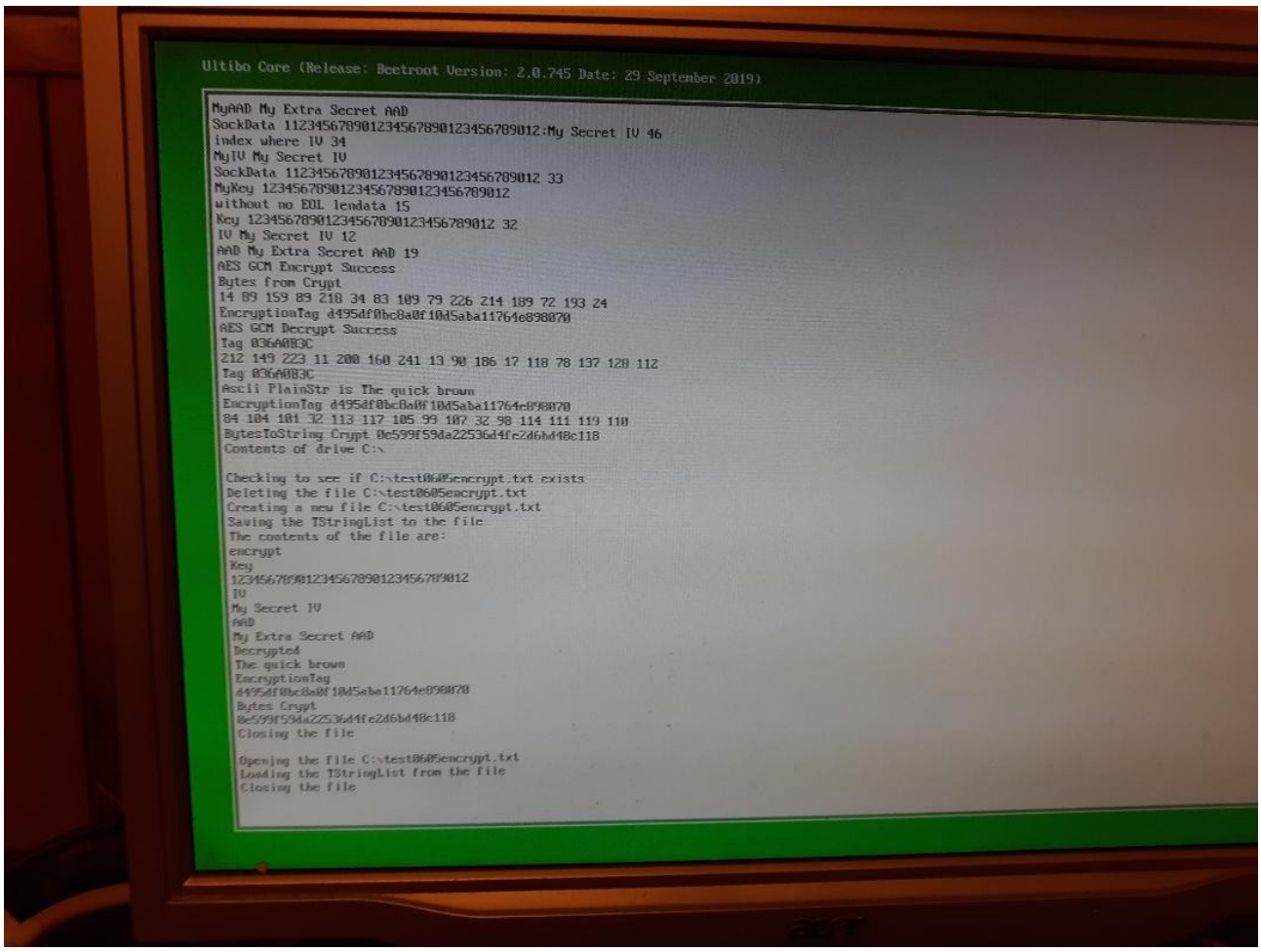
The initial values were below.
MyKey: AnsiString = '1234567890123456'; {Must be 16, 24 or 32 bytes}
MyIV: AnsiString = 'My Secret IV';
MyAAD: AnsiString = 'My Extra Secret AAD';
MyData: AnsiString = 'The quick brown fox jumps over the lazy dog.The quick brown fox jumps over the lazy dog.';

when the string below is sent to the Ultibo System

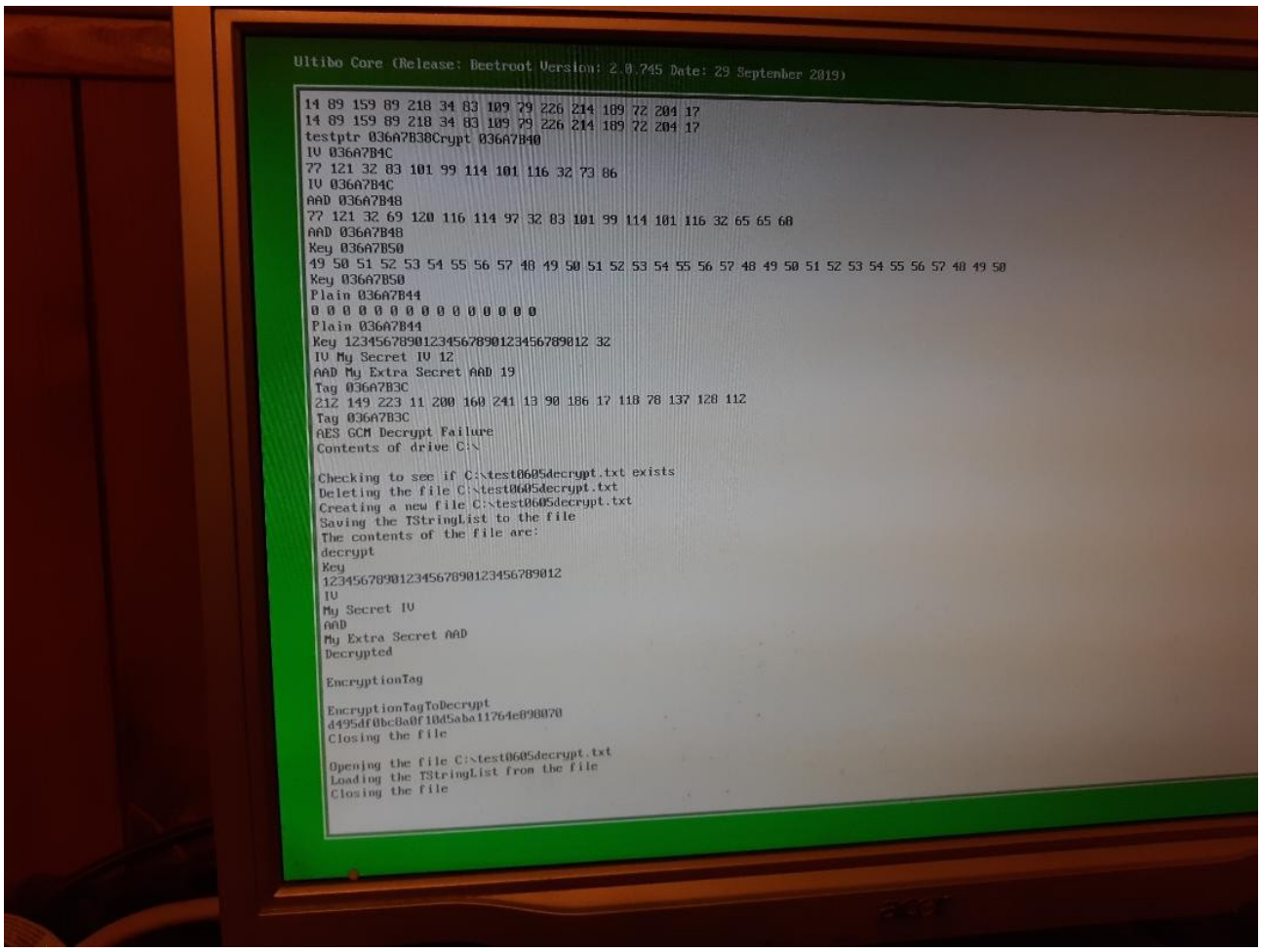
telnet 192.168.1.245 5050
Trying 192.168.1.245...
Connected to 192.168.1.245.
Escape character is '^]'.
112345678901234567890123456789012:My Secret IV:My Extra Secret AAD:The quick brown
112345678901234567890123456789012:My Secret IV:My Extra Secret AAD:The quick brown
testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz

The results are writen to file test0603.txt

tftp 192.168.1.245
tftp> binary



256 Bit decrypt



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

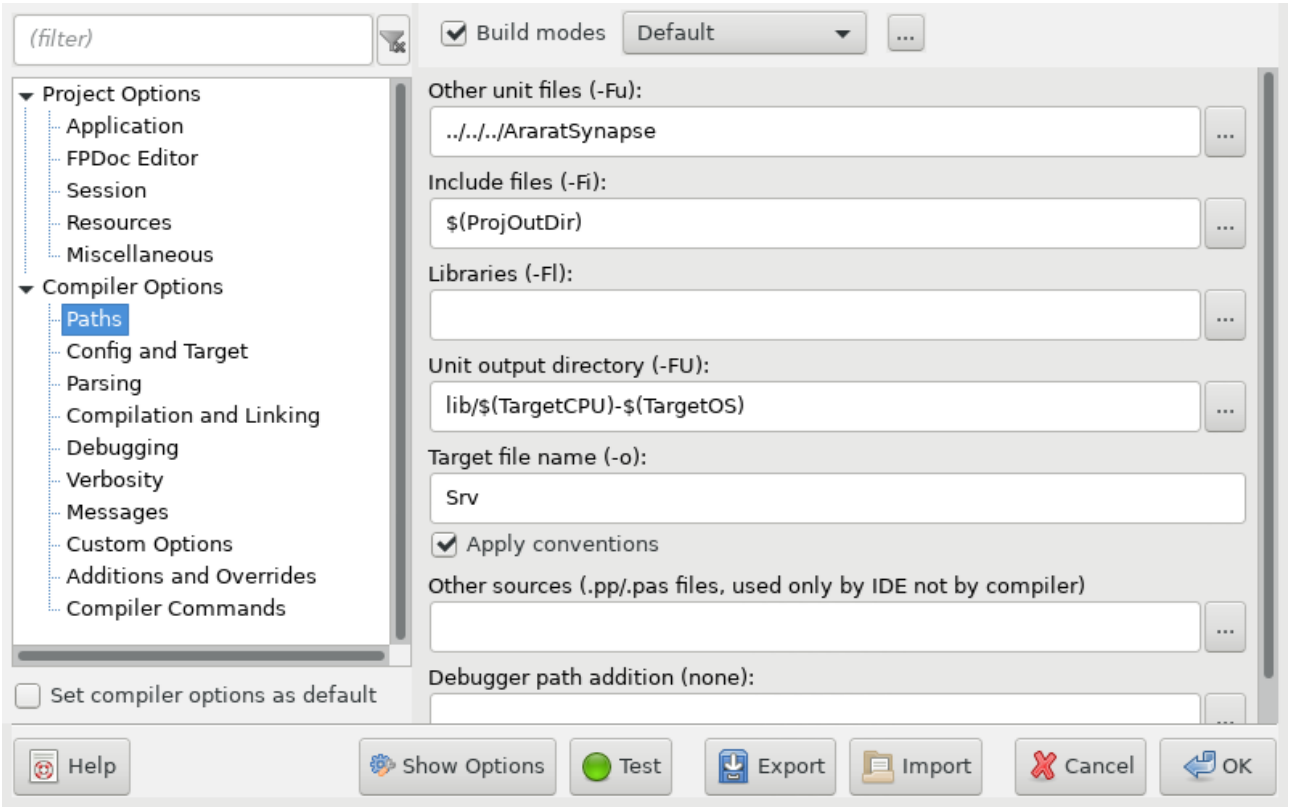
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI3B -Fu../../../AraratSynapse @/home/devel/ultibo/core/fpc/bin/RPI3.CFG -O2 Srv.lpr

or

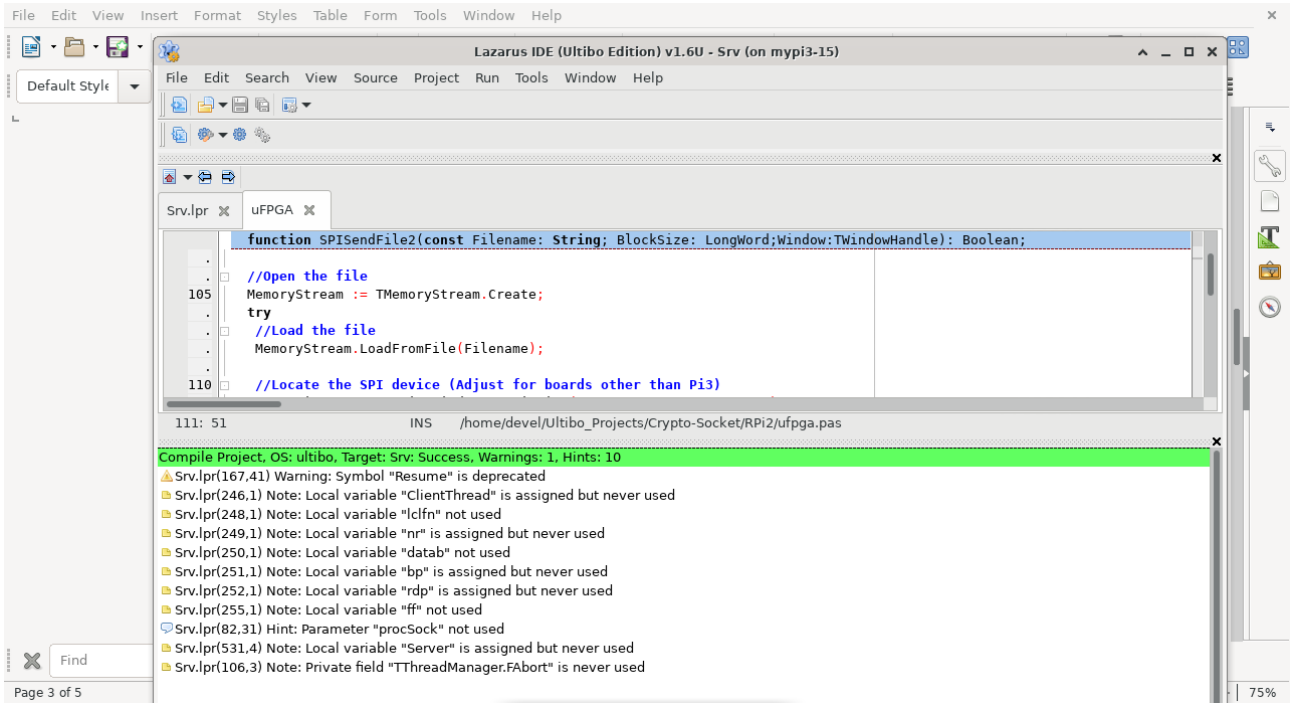
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI2B -Fu../../../AraratSynapse
@/home/devel/ultibo/core/fpc/bin/RPI2.CFG -O2 Srv.lpr
Transfer kernel7.img

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

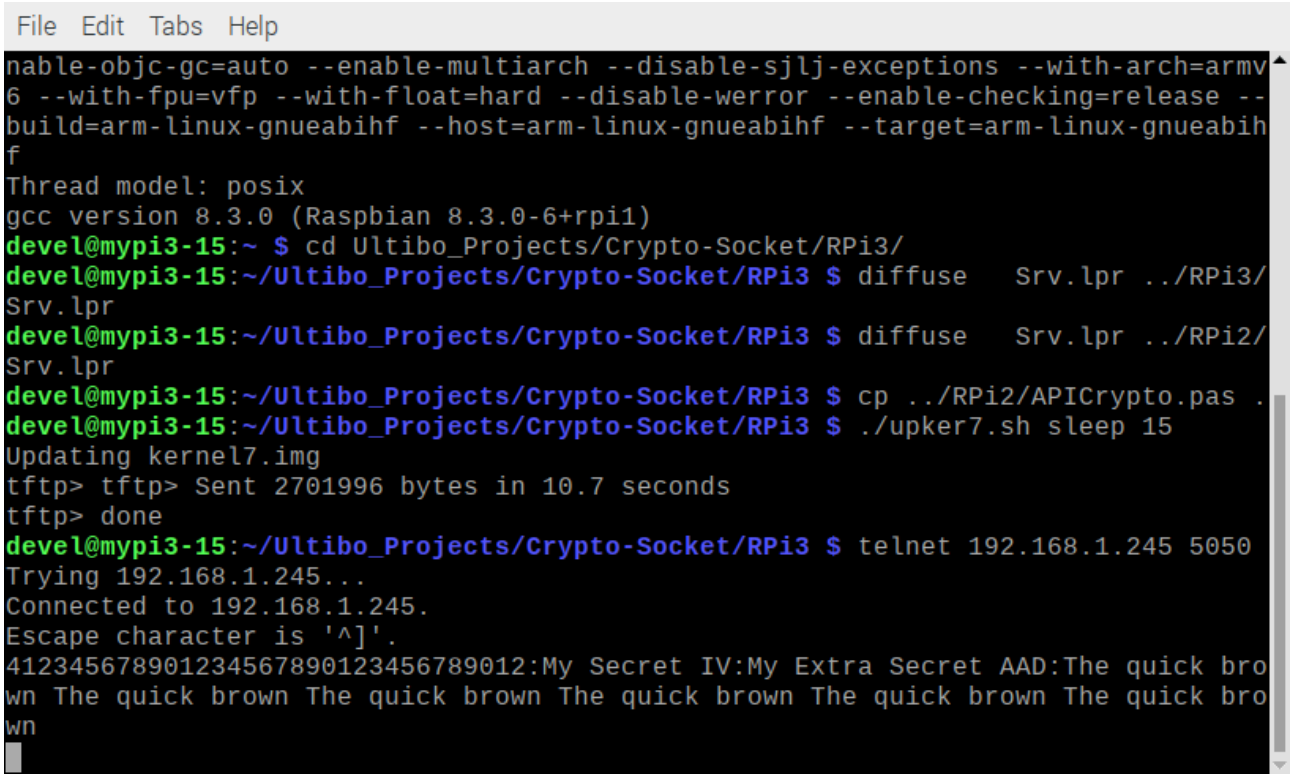
Compiling with Lazaraus.



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