KryptoMessage3.js 25 Aug 2016

For use on Espruino Pico device

Requires: RBG.js, AEScmac.js, permutation.js (see post above for files)

FlashEEPROM.js from Espruino web site.

Uses serial port 1 (can be changed in configuration at top) in a hardware loopback.

Connect pins B6 and B7 together.

Reads analog input on Pin B1.

There are a number of flag variables at the top of the program:

Flag to suppress server text to console:

var showserver=0;

//var showserver=1;

Where to get the cryptographic keys:

//var KeysFromRom=0; //Generate keys as before this point

var KeysFromRom=1;//read keys from ROM see previous post for the key generator and squirt programs to insert the keys into the EEROM

Serial port parameters:

//var useserialflag=0;

var useserialflag=1;

var baudrate=115200;

var Port=Serial1;

Flags used in the Msg transport function:

//var EncryptionFlag=false;

var EncryptionFlag=true;

//var PermutationFlag=false;

var PermutationFlag=true;

ReplayFlag controls the recording of msgs for replay:

var ReplayFlag=true;

//var ReplayFlag=false;

This version redirects the console in order to create a menu on the USB port to that the program can be operated from a terminal program or from the left pane of the WebIDE.

BE SURE TO TYPE 0 TO MAKE THE RUNNING PROGRAM RESTORE THE CONSOLE TO THE USB PORT! This will avoid having to reset the PICO by cycling the power.

The Menu:

Xxx

Select using digit and return key

1 Connect 6 Cshow

2 Logoff 7 LEDon

3 Creplay 8 LEDoff

4 Creset 9 Read ADC

5 Sshow 0 Exit

Xxx

Connect starts the client to server connection.

It asks for the User ID and Password Id= Sam, PW= 1234

(unless you change these in the key generator program)

Logoff tells the server that connect will be needed for access.

Creplay is used after a session to replay client messages for testing

Creset resets the replay buffers

Sshow prints the recorded server messages

Cshow prints the recorded client messages

LEDon, LEDoff operate the LED on the PICO.

Read Adc reads a 0 to 4096 (12 bits) value from pin B1.

And finally Exit restores the console to the USB port.

/\*

Todo add0x32 message if wrong Id and password

Todo rework PICO commands into a User client and server functions

Todo add code for lexlevel 1 to generate keys on the client and send them to the server

Todo split into server and client versions on two different PICOs

Todo connect server and client PICOs using serial port

\*/

/\*

Done see if serial1 and serial2 on PICO can be used to connect

 the server and client portions of this program

 Solution use serial1 in loopback with flag

Done write a program that generates keys and writes the to ROM

Done read the keys from the ROM

Done add 0x30 and 0x31 code for server bad msg, client not authentic

Done add blend function to msg send and recieve functions

Done add code to do menu on USB allows terminal program to operate

\*/

Xxxx

Select using digit and return key

1 Connect 6 Cshow

2 Logoff 7 LEDon

3 Creplay 8 LEDoff

4 Creset 9 Read ADC

5 Sshow 0 Exit

<- USB

>1

do connect

 Client builds and sends inital message

Permutated Encrypted Message=

60,d4,88,53,63,4e,c1,43,d,94,61,c,e6,37,14,e8,

a3,68,bd,c0,cd,c0,2a,e8,a4,3a,7e,aa,dd,82,91,4f,

1d,66,74,41,b7,90,45,97,7,51,13,8e,ab,7f,2c,c,

45,2,e3,4f,e3,8e,c3,aa,ec,a6,e1,f9,ab,c7,4f,93,

3b,a6,a7,61,14,3b,25,90,9b,32,4f,d4,54,70,f,d8,

Enter User ID

process server

decrypt

Server replies to connect message

Permutated Encrypted Message=

8b,cf,f9,2b,85,10,79,ca,9d,3d,c9,80,19,c4,ed,5b,

2,bf,c0,5,74,fb,9e,2f,88,5f,c5,11,ba,8d,31,51,

9,e9,78,90,24,e0,35,8c,e6,a7,eb,de,69,b8,57,9a,

19,f1,f1,9f,ee,f9,6e,48,e1,d9,3a,8c,1a,7e,bc,68,

33,7b,3a,e2,39,b4,a3,61,ca,98,fd,aa,ec,d8,6f,a5,

server transmits

process client 80

decrypt

 Client checks the server message

Client check of server msg OK

Client checks if the server is authentic

Server is Authentic

Enter User ID

Sam

Enter Password

1234

Login using Sam and 1234

Client login message

Permutated Encrypted Message=

1f,f0,25,77,2,b5,d0,13,cf,63,8e,b9,ef,fe,95,e8,

73,ae,f9,88,a3,d4,0,56,32,d5,f9,c0,4c,6,5b,d9,

7c,e4,c,ef,64,ee,2c,a3,cf,dc,c3,86,d3,f,2f,3f,

57,c4,98,31,b6,ad,47,81,3a,21,ae,3f,90,22,57,69,

7c,d0,da,0,54,88,34,7c,f0,5f,ef,a0,c5,a7,e,ab,

process server

decrypt

Permutated Encrypted Message=

63,28,3e,c4,c5,3,b5,f0,7d,66,81,c8,74,99,5e,4f,

6,a3,46,29,49,a5,e,bf,79,b7,64,4f,98,4c,c4,34,

75,46,7c,7c,5e,a0,1f,af,32,9d,e6,13,2b,66,b9,18,

54,32,83,19,63,ff,3e,f1,de,ab,77,ab,f,f2,65,fb,

d8,f0,49,e9,80,16,ee,e7,b,bd,fd,63,4d,48,49,e7,

server transmits

process client 80

decrypt

 Client checks the server message

Client check of server msg OK

Client checks if the server is authentic

Server is Authentic

Client sees msg 0x42

Select using digit and return key

1 Connect 6 Cshow

2 Logoff 7 LEDon

3 Creplay 8 LEDoff

4 Creset 9 Read ADC

5 Sshow 0 Exit

xxxxxx