DAVID RICARDO CRUZ JUAREZ

EL ARCUIVO “helloword” es el main en cada proyecto

EJECUCION DE implementación de los algoritmos de SHA512 tarjeta OKDo.

*/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/*

*/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* PASS WORD PARA UN HASH DE SHA 512 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/*

#include "fsl\_device\_registers.h"

#include "fsl\_debug\_console.h"

#include "pin\_mux.h"

#include "clock\_config.h"

#include "board.h"

#include "fsl\_power.h"

#include "mbedtls/platform.h"

#include "mbedtls/platform\_util.h"

#include "mbedtls/sha512.h"

*// Digest prealmacenado de la contraseña "HASH DE SHA-512 "*

*// LA CONTRASEÑA ES HELLODAVE*

const unsigned char correct\_password\_digest**[**64**]** **=** **{**

0xE6**,**0x10**,**0xE4**,**0x4D**,**0x54**,**0xE8**,**0x79**,**0x0**,**0xB6**,**0x6**,**0x67**,**

0x81**,**0xEA**,**0xEF**,**0xF2**,**0x46**,**0x8**,**0xF3**,**0xF5**,**0x53**,**0xC3**,**0xC3**,**

0x43**,**0xF6**,**0x51**,**0x5C**,**0x8D**,**0xA4**,**0xB8**,**0x39**,**0xC2**,**0xE3**,**0xBE**,**

0x34**,**0xD**,**0x40**,**0xFB**,**0x25**,**0x8D**,**0xDC**,**0x9**,**0x59**,**0xC9**,**0xFC**,**

0x8A**,**0x8D**,**0xEE**,**0x8F**,**0x2E**,**0x4B**,**0x27**,**0x68**,**0xF4**,**0x4A**,**0x9E**,**

0x90**,**0x9F**,**0xCC**,**0x31**,**0xD0**,**0x47**,**0x4**,**0xC8**,**0xAE**};**

#define BUF\_SIZE 128

#define SHA512\_SIZE 64

unsigned char sha512sum**[**SHA512\_SIZE**];**

*// Inicialización del contexto de SHA-512*

mbedtls\_sha512\_context sha512\_ctx**;**

void resetPasswordBuffer**(**char **\***buffer**,** size\_t size**)**

**{**

**for** **(**size\_t i **=** 0**;** i **<** size**;** **++**i**)**

**{**

buffer**[**i**]** **=** '\0'**;**

**}**

**}**

void calculateSHA512**(**const char **\***input**,** size\_t size**,** unsigned char **\***output**)**

**{**

mbedtls\_sha512\_starts\_ret**(&**sha512\_ctx**,** 0**);**

mbedtls\_sha512\_update\_ret**(&**sha512\_ctx**,** **(**const unsigned char **\*)**input**,** size**);**

mbedtls\_sha512\_finish\_ret**(&**sha512\_ctx**,** output**);**

**}**

int compareDigests**(**const unsigned char **\***digest1**,** const unsigned char **\***digest2**,** size\_t size**)**

**{**

**for** **(**size\_t i **=** 0**;** i **<** size**;** **++**i**)**

**{**

**if** **(**digest1**[**i**]** **!=** digest2**[**i**])**

**{**

**return** 0**;** *// No son iguales*

**}**

**}**

**return** 1**;** *// Son iguales*

**}**

int main**(**void**)**

**{**

char ch**;**

char passwordBuffer**[**BUF\_SIZE**];**

unsigned char userPasswordDigest**[**SHA512\_SIZE**];**

*/\* Inicialización del hardware y configuraciones iniciales \*/*

POWER\_SetBodVbatLevel**(**kPOWER\_BodVbatLevel1650mv**,** kPOWER\_BodHystLevel50mv**,** false**);**

CLOCK\_AttachClk**(**BOARD\_DEBUG\_UART\_CLK\_ATTACH**);**

BOARD\_InitBootPins**();**

BOARD\_InitBootClocks**();**

BOARD\_InitDebugConsole**();**

CRYPTO\_InitHardware**();**

*// Inicialización del contexto SHA-512*

mbedtls\_sha512\_init**(&**sha512\_ctx**);**

**while** **(**1**)**

**{**

resetPasswordBuffer**(**passwordBuffer**,** BUF\_SIZE**);**

PRINTF**(**"Ingrese la contraseña: "**);**

uint8\_t index **=** 0**;**

**while** **(**1**)**

**{**

ch **=** GETCHAR**();**

**if** **(**ch **==** '\r' **||** index **>=** BUF\_SIZE **-** 1**)**

**{**

**break;**

**}**

PUTCHAR**(**'\*'**);** *// Muestra "\*" en lugar del caracter real para mayor seguridad*

passwordBuffer**[**index**++]** **=** ch**;**

**}**

*// Calcula el hash SHA-512 de la contraseña ingresada*

calculateSHA512**(**passwordBuffer**,** index**,** userPasswordDigest**);**

*// Compara el hash de la contraseña ingresada con el digest prealmacenado*

**if** **(**compareDigests**(**userPasswordDigest**,** correct\_password\_digest**,** SHA512\_SIZE**))**

**{**

PRINTF**(**"\n\rContraseña correcta. Acceso concedido.\r\n"**);**

**}**

**else**

**{**

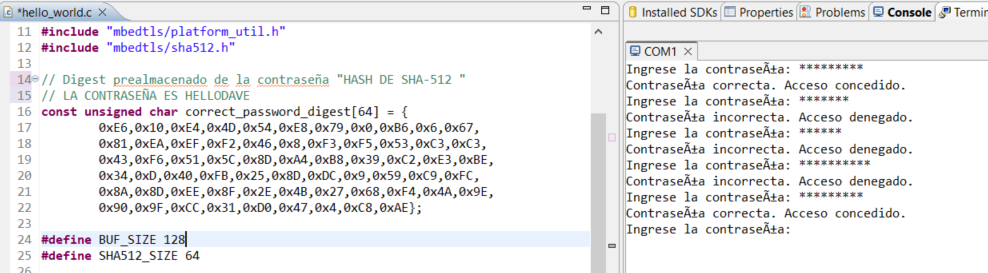
PRINTF**(**"\n\rContraseña incorrecta. Acceso denegado.\r\n"**);**

**}**

**}**

**}**

RESULTADO DE SHA 512 VERIFICANDO HASH



EJECUCION DE implementación de los algoritmos de SHA256 en la tarjeta OKDo.

*/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/*

*/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* PASS WORD PARA UN HASH SHA 256 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/*

#include "fsl\_device\_registers.h"

#include "fsl\_debug\_console.h"

#include "pin\_mux.h"

#include "clock\_config.h"

#include "board.h"

#include "fsl\_power.h"

#include "mbedtls/platform.h"

#include "mbedtls/platform\_util.h"

#include "mbedtls/sha256.h"

*// Digest prealmacenado de la contraseña "SHA 256 HASH" LA CONTRASEÑA ES HELLODAVE*

const unsigned char correct\_password\_digest**[**32**]** **=** **{**

0xB9**,**0xBA**,**0xF6**,**0x3C**,**0x97**,**0xB6**,**0x86**,**0x4C**,**0x8**,**

0xAE**,**0x50**,**0xD5**,**0xE6**,**0xEE**,**0xD6**,**0x62**,**0x66**,**0x8E**,**

0x19**,**0xBB**,**0x9C**,**0x19**,**0x8F**,**0xDF**,**0x21**,**0x7F**,**0x26**,**

0x9A**,**0x91**,**0xC3**,**0x24**,**0x83

**};**

#define BUF\_SIZE 128

#define SHA256\_SIZE 32

unsigned char sha256sum**[**SHA256\_SIZE**];**

*// Inicialización del contexto de SHA-256*

mbedtls\_sha256\_context sha256\_ctx**;**

void resetPasswordBuffer**(**char **\***buffer**,** size\_t size**)**

**{**

**for** **(**size\_t i **=** 0**;** i **<** size**;** **++**i**)**

**{**

buffer**[**i**]** **=** '\0'**;**

**}**

**}**

void calculateSHA256**(**const char **\***input**,** size\_t size**,** unsigned char **\***output**)**

**{**

mbedtls\_sha256\_starts\_ret**(&**sha256\_ctx**,** 0**);**

mbedtls\_sha256\_update\_ret**(&**sha256\_ctx**,** **(**const unsigned char **\*)**input**,** size**);**

mbedtls\_sha256\_finish\_ret**(&**sha256\_ctx**,** output**);**

**}**

int compareDigests**(**const unsigned char **\***digest1**,** const unsigned char **\***digest2**,** size\_t size**)**

**{**

**for** **(**size\_t i **=** 0**;** i **<** size**;** **++**i**)**

**{**

**if** **(**digest1**[**i**]** **!=** digest2**[**i**])**

**{**

**return** 0**;** *// No son iguales*

**}**

**}**

**return** 1**;** *// Son iguales*

**}**

int main**(**void**)**

**{**

char ch**;**

char passwordBuffer**[**BUF\_SIZE**];**

unsigned char userPasswordDigest**[**SHA256\_SIZE**];**

*/\* Inicialización del hardware y configuraciones iniciales \*/*

POWER\_SetBodVbatLevel**(**kPOWER\_BodVbatLevel1650mv**,** kPOWER\_BodHystLevel50mv**,** false**);**

CLOCK\_AttachClk**(**BOARD\_DEBUG\_UART\_CLK\_ATTACH**);**

BOARD\_InitBootPins**();**

BOARD\_InitBootClocks**();**

BOARD\_InitDebugConsole**();**

CRYPTO\_InitHardware**();**

*// Inicialización del contexto SHA-256*

mbedtls\_sha256\_init**(&**sha256\_ctx**);**

**while** **(**1**)**

**{**

resetPasswordBuffer**(**passwordBuffer**,** BUF\_SIZE**);**

PRINTF**(**"Ingrese la contraseña: "**);**

uint8\_t index **=** 0**;**

**while** **(**1**)**

**{**

ch **=** GETCHAR**();**

**if** **(**ch **==** '\r' **||** index **>=** BUF\_SIZE **-** 1**)**

**{**

**break;**

**}**

PUTCHAR**(**'\*'**);** *// Muestra "\*" en lugar del caracter real para mayor seguridad*

passwordBuffer**[**index**++]** **=** ch**;**

**}**

*// Calcula el hash SHA-256 de la contraseña ingresada*

calculateSHA256**(**passwordBuffer**,** index**,** userPasswordDigest**);**

*// Compara el hash de la contraseña ingresada con el digest prealmacenado*

**if** **(**compareDigests**(**userPasswordDigest**,** correct\_password\_digest**,** SHA256\_SIZE**))**

**{**

PRINTF**(**"\n\rContraseña correcta. Acceso concedido.\r\n"**);**

**}**

**else**

**{**

PRINTF**(**"\n\rContraseña incorrecta. Acceso denegado.\r\n"**);**

**}**

**}**

**}**

RESULTADO DE ESA EJECUCION

