Ejecución del Código de cifrado MD5, SHA-1, SHA-256, SHA-512

/\*

\* Copyright (c) 2013 - 2015, Freescale Semiconductor, Inc.

\* Copyright 2016-2017 NXP

\* All rights reserved.

\*

\* SPDX-License-Identifier: BSD-3-Clause

\*/

#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 "ksdk\_mbedtls.h"

#include "mbedtls/md5.h"

#include "mbedtls/sha1.h"

#include "mbedtls/sha256.h"

#include "mbedtls/sha512.h"

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

*\* Definitions*

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

#define BUF\_SIZE 128

#define MD5\_SIZE 16

#define SHA1\_SIZE 20

#define SHA256\_SIZE 32

#define SHA512\_SIZE 64

/\*DWT - Data Watchpoint and Trace Unit, Cycle count register\*/

#define Init\_cycle\_counter() DWT->CTRL |= DWT\_CTRL\_EXCTRCENA\_Msk

#define Reset\_timer() DWT->CYCCNT = 0

#define Enable\_cycle\_counter() DWT->CTRL |= DWT\_CTRL\_CYCCNTENA\_Msk

#define Disable\_cycle\_counter() DWT->CTRL &= ~DWT\_CTRL\_CYCCNTENA\_Msk

#define Get\_cycle\_counter() DWT->CYCCNT

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

*\* Prototypes*

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

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

*\* Code*

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

*/\*!*

*\* @brief Main function*

*\*/*

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

**{**

char ch**;**

unsigned char buff**[**BUF\_SIZE**];**

unsigned char index **=** 0**,** i**;**

unsigned char md5sum**[**MD5\_SIZE**];**

unsigned char sha1sum**[**SHA1\_SIZE**];**

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

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

uint32\_t u32cycles**;**

mbedtls\_sha1\_context ctx**;**

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

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

*/\* Init board hardware. \*/*

*/\* set BOD VBAT level to 1.65V \*/*

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

*/\* attach main clock divide to FLEXCOMM0 (debug console) \*/*

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

BOARD\_InitBootPins**();**

BOARD\_InitBootClocks**();**

BOARD\_InitDebugConsole**();**

CRYPTO\_InitHardware**();**

#if !defined(DONT\_ENABLE\_FLASH\_PREFETCH)

*/\* enable flash prefetch for better performance \*/*

SYSCON**->**FMCCR **|=** SYSCON\_FMCCR\_PREFEN\_MASK**;**

#endif

Init\_cycle\_counter**();**

Reset\_timer**();**

Enable\_cycle\_counter**();**

PRINTF**(**"My HASHING\r\n"**);**

mbedtls\_sha1\_init**(** **&**ctx **);**

mbedtls\_sha256\_init**(** **&**ctx **);**

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

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

**{**

index **=** 0**;**

ch **=** '\0'**;**

PRINTF**(**"Input Buffer: "**);**

**while(**ch **!=** '\r' **&&** index **<** BUF\_SIZE**)**

**{**

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

PUTCHAR**(**ch**);**

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

**}**

Reset\_timer**();**

mbedtls\_md5\_ret**(**buff**,**index **-** 1**,** md5sum **);**

u32cycles **=** Get\_cycle\_counter**();**

PRINTF**(**"\n\rMD5: "**);**

**for(**i**=**0**;**i**<**MD5\_SIZE**;**i**++)**

**{**

PRINTF**(**" 0x%X"**,** md5sum**[**i**]);**

**}**

PRINTF**(**"\r\nCycles: %d \r\n"**,**u32cycles**);**

*/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* SHA-1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/*

Reset\_timer**();**

mbedtls\_sha1\_starts\_ret**(** **&**ctx **);**

mbedtls\_sha1\_update\_ret**(** **&**ctx**,** buff**,** index **-** 1 **);**

mbedtls\_sha1\_finish\_ret**(** **&**ctx**,** sha1sum **);**

mbedtls\_sha1\_free**(** **&**ctx **);**

u32cycles **=** Get\_cycle\_counter**();**

PRINTF**(**"\n\rSHA1: "**);**

**for(**i**=**0**;**i**<**SHA1\_SIZE**;**i**++)**

**{**

PRINTF**(**" 0x%X"**,** sha1sum**[**i**]);**

**}**

PRINTF**(**"\r\nCycles: %d \r\n"**,**u32cycles**);**

*/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* SHA-256 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/*

Reset\_timer**();**

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

mbedtls\_sha256\_update\_ret**(&**sha256\_ctx**,** buff**,** index **-** 1**);**

mbedtls\_sha256\_finish\_ret**(&**sha256\_ctx**,** sha256sum**);**

u32cycles **=** Get\_cycle\_counter**();**

PRINTF**(**"\n\rSHA256: "**);**

**for** **(**i **=** 0**;** i **<** SHA256\_SIZE**;** i**++)**

**{**

PRINTF**(**" 0x%X"**,** sha256sum**[**i**]);**

**}**

PRINTF**(**"\r\nCycles: %d \r\n"**,** u32cycles**);**

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

*/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* SHA-512 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/*

Reset\_timer**();**

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

mbedtls\_sha512\_update\_ret**(&**sha512\_ctx**,** buff**,** index **-** 1**);**

mbedtls\_sha512\_finish\_ret**(&**sha512\_ctx**,** sha512sum**);**

u32cycles **=** Get\_cycle\_counter**();**

PRINTF**(**"\n\rSHA512: "**);**

**for** **(**i **=** 0**;** i **<** SHA512\_SIZE**;** i**++)**

**{**

PRINTF**(**" 0x%X"**,** sha512sum**[**i**]);**

**}**

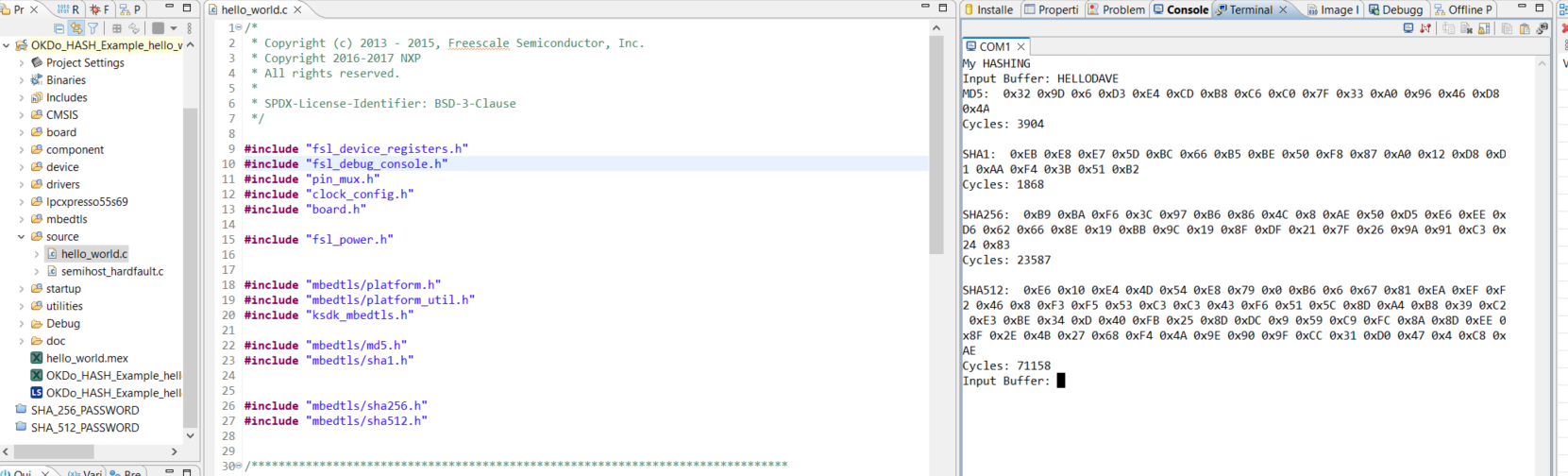
PRINTF**(**"\r\nCycles: %d \r\n"**,** u32cycles**);**

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

**}**

**}**

RESULTADO EN CONSOLA



Anexe archivo.txt con los hash de la contraseña