Ryan Sewell

CpE301

February 24, 2025

Design Assignment 1

; DesignAssignment1.asm

;

; Created: 2/17/2025 12:12:03 PM

; Author : Ryan Sewell

;

; Define constants

.equ DELTA = 0x9E3779B9

.equ NUM\_ROUNDS = 32

; Define EEPROM addresses

.equ KEY\_EEPROM = 0x0000

; Define program memory addresses

.equ PLAINTEXT\_START = 0x0400

.equ ENCRYPTED\_START = 0x8000

; Define registers

.def R\_V0 = R16

.def R\_V1 = R17

.def R\_SUM = R18

.def R\_DELTA = R19

.def R\_ROUNDS = R20

.def R\_KEY0 = R21

.def R\_KEY1 = R22

.def R\_KEY2 = R23

.def R\_KEY3 = R24

; Load key from EEPROM to registers

LDI ZH, HIGH(KEY\_EEPROM)

LDI ZL, LOW(KEY\_EEPROM)

LD R\_KEY0, Z+

LD R\_KEY1, Z+

LD R\_KEY2, Z+

LD R\_KEY3, Z+

; Initialize pointers

LDI XL, LOW(PLAINTEXT\_START)

LDI XH, HIGH(PLAINTEXT\_START)

LDI YL, LOW(ENCRYPTED\_START)

LDI YH, HIGH(ENCRYPTED\_START)

; Main encryption loop

ENCRYPT\_LOOP:

; Load plaintext block

LD R\_V0, X+

LD R\_V1, X+

; Initialize sum and rounds

CLR R\_SUM

LDI R\_ROUNDS, NUM\_ROUNDS

; TEA encryption rounds

TEA\_ROUND:

; V0 += ((V1 << 4) + K0) ^ (V1 + SUM) ^ ((V1 >> 5) + K1)

MOV R25, R\_V1

LSL R\_V1

ADD R\_V1, R\_KEY0

ADD R\_V1, R\_SUM

LSR R25

ADD R25, R\_KEY1

EOR R\_V0, R25

; V1 += ((V0 << 4) + K2) ^ (V0 + SUM) ^ ((V0 >> 5) + K3)

MOV R26, R\_V0

LSL R\_V0

ADD R\_V0, R\_KEY2

ADD R\_V0, R\_SUM

LSR R26

ADD R26, R\_KEY3

EOR R\_V1, R26

; SUM += DELTA

LDI R25, LOW(DELTA)

LDI R26, HIGH(DELTA)

ADD R\_SUM, R25

ADC R\_SUM, R26

; Decrement rounds and check if done

DEC R\_ROUNDS

BRNE TEA\_ROUND

; Store encrypted block

ST Y+, R\_V0

ST Y+, R\_V1

; Check if all blocks are encrypted

CPI XL, HIGH(PLAINTEXT\_START + 64)

BRNE ENCRYPT\_LOOP

END:

RJMP END

LOAD\_FROM\_EEPROM:

SBIC EECR, EEPE

RJMP LOAD\_FROM\_EEPROM

OUT EEARH,XH

OUT EEARL,XL

SBI EECR,EERE

IN R20,EEDR

RET

STORE\_IN\_EEPROM:

SBIC EECR, EEPE

RJMP STORE\_IN\_EEPROM

OUT EEARH,XH

OUT EEARL,XL

OUT EEDR,R20

SBI EECR,EEMPE

SBI EECR,EEPE

RET

; Message: "jiLSTLNdaRrxrmiElGjSeiZBNSIrXEOInKAljICoLQvnCSTuTqApIrpqhyjBNAYy"

.ORG 0x200

MESSAGE: .DB 0x6a, 0x69, 0x4c, 0x53, 0x54, 0x4c, 0x4e, 0x64, 0x61, 0x52, 0x72, 0x78, 0x72, 0x6d, 0x69, 0x45

;.DB 6c, 47, 6a, 53, 65, 69, 5a, 42, 4e, 53, 49, 72, 58, 45, 4f, 49

;.DB 6e, 4b, 41, 6c, 6a, 49, 43, 6f, 4c, 51, 76, 6e, 43, 53, 54, 75

;.DB 54, 71, 41, 70, 49, 72, 70, 71, 68, 79, 6a, 42, 4e, 41, 59, 79

; KEY: "YKTFgWnvaloBflrr"

.ORG 0x300

KEY:.DB 0x59, 0x4b, 0x54, 0x46, 0x67, 0x57, 0x6e, 0x76, 0x61, 0x6c, 0x6f, 0x42, 0x66, 0x6c, 0x72, 0x72

A close-up of a computer screen

AI-generated content may be incorrect.