LibEncDec
加解密接口库说明书

辰星科技
ORISTAR

Version	Date	Modify	Review	Remark
V0.1	2017-06-17	张绍言	孙鹏	初稿

数码辰星科技发展（北京）有限公司

CONTENTS

■接口库文件说明

文件名	说明
libencdec.h	头文件
LibEncDec.lib	由 MDK-ARM 工具链编译生成的 lib 文件
test.c	测试程序

■接口函数说明

序号	函数接口说明

1
获取版本号
	//function:used to get the libencdec version number.
	//arg1: major,a byte buffer to hold the major number.
	//arg2: minor,a byte buffer to hold the minor number.
	//ret: 0,success. -1,error.
	int tc_get_version(char *major,char *minor);

2
更新密钥
	//function:used to update the security key.
	//arg1: keyData,the new security key.
	//arg2: keySize,the new key size,must be 16 bytes.
	//ret: 0,success. -1,error.
	int tc_update_key(const char* keyData, int keySize);

3
加密函数
	//function:used to encrypt data.
	//arg1: srcData,the plain data.
	//arg2: srcSize,the plain data size,must be aligned by 8 bytes.
	//arg3: dstData,the buffer to hold the encrypted data.
	//arg4: dstSize,the buffer size,must be greater or equal than srcSize.
	//ret: 0,success. -1,error.
	int tc_enc(const char *srcData, int srcSize, char *dstData, int dstSize);

4
解密函数
	//function:used to encrypt data.
	//arg1: srcData,the plain data.
	//arg2: srcSize,the plain data size,must be aligned by 8 bytes.
	//arg3: dstData,the buffer to hold the encrypted data.
	//arg4: dstSize,the buffer size,must be greater or equal than srcSize.
	//ret: 0,success. -1,error.
	int tc_dec(const char *srcData, int srcSize, char *dstData, int dstSize);

■加解密说明

因接口库使用的是块加密算法，以 8 字节为一个基本的运算单位，所以加密或解密的源数据大小必须保证 8 字节对齐，对于不满足要求的数据，请在协议中填充 1~7 个 0 数据补齐。

密钥的长度固定为 16 个字节。

接口库使用过程中，请严格检测函数的返回值，来判断执行结果是成功还是失败。

■滚动密钥机制

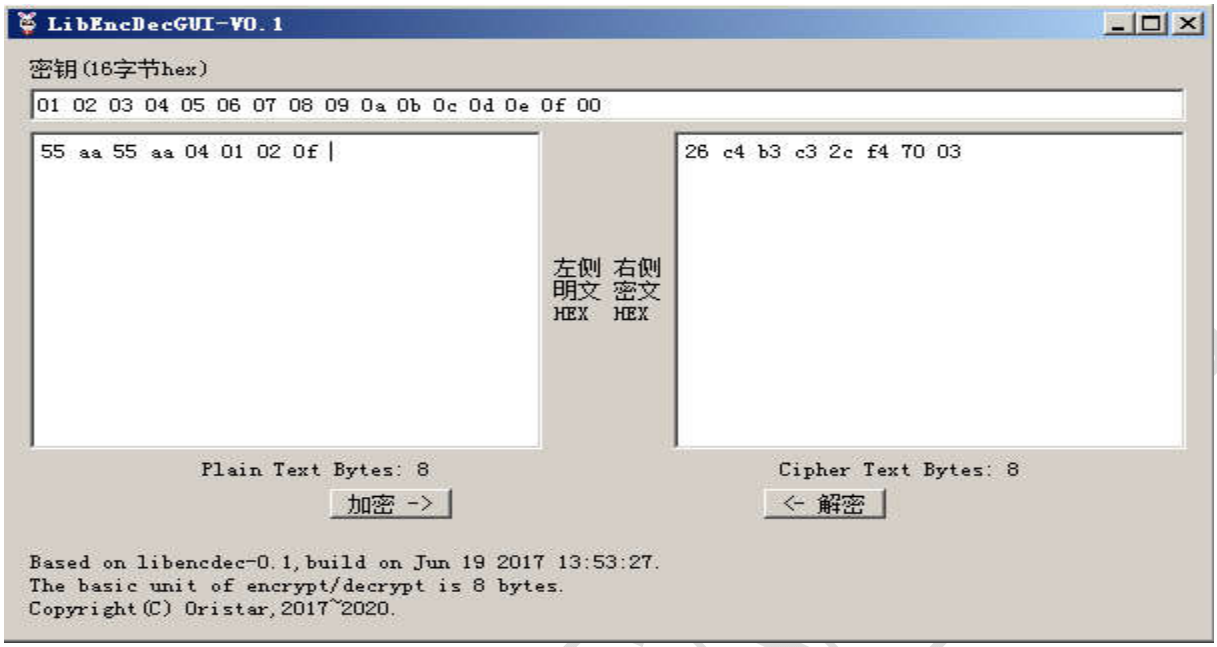
接口库有初始的密钥，在设备开机上电时，将使用初始密钥进行加解密操作。通信过程中，由 Master 设备周期性的请求更新 Slave 设备的密钥，Slave 收到密钥并正确应答 Master 后，双方使用新的密钥进行通信，否则，依旧使用老密钥通信。密钥的随机生成规则及更新频率由 Master 决定。

■测试 Demo

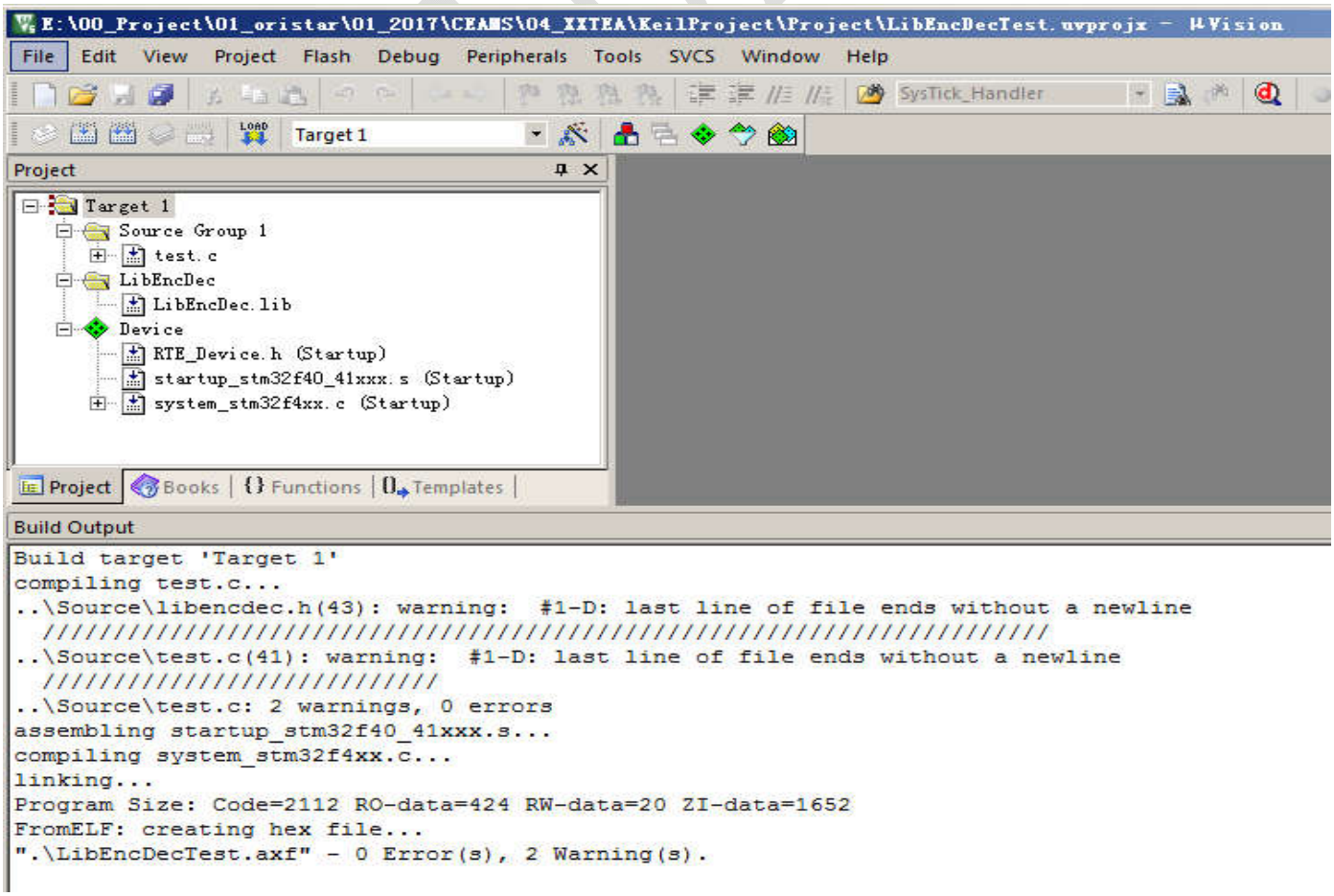
```
#include "libencdec.h"
int main(void)
{
    int ret;
    char version[2];
    char newKey[16]={0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,
                     0x08,0x09,0x0a,0x0b,0x0c,0x0d,0x0e,0x0f};
    char plainData[8]={0x01,0x11,0x5C,0xBC,0xAA,0x55,0x93,0x81};
    char encryptData[8];
    char decryptData[8];
    //get libencdec version.
    ret=tc_get_version(&version[0],&version[1]);
    if(ret<0)
    {
       //error handle.
    }
    //use new security key to do encrypt&decrypt.
    ret=tc_update_key(newKey,sizeof(newKey));
    if(ret<0)
    {
        //error handle.
    }
    //do encrypt.
    ret=tc_enc(plainData,sizeof(plainData),encryptData,sizeof(encryptData));
```

```
    if(ret<0)
    {
        //error handle.
    }
    //do decrypt.
    ret=tc_dec(encryptData,sizeof(encryptData),decryptData,sizeof(decryptData));
    if(ret<0)
    {
        //error handle.
    }
    return 0;
}
```

■验证测试工具



■Keil 工程使用



■版本发布记录

版本号	时间	说明	发布文件
V0.1	2017-06-17	最初版本	libencdec-0.1.for.mdk.5.11.rar

********** THE END OF FILE **********