软体实作 DES

NuMicro® 32 位系列微控制器范例代码介绍

文件信息

代码简述	用软体实作 Data Encryption Standard 算法
BSP 版本	NUC230/240 Series BSP v3.01.002
开发平台	NuTiny–EVB–NUC240–LQFP100 V1.0

The information described in this document is the exclusive intellectual property of Nuvoton Technology Corporation and shall not be reproduced without permission from Nuvoton.

Nuvoton is providing this document only for reference purposes of NuMicro microcontroller based system design. Nuvoton assumes no responsibility for errors or omissions.

All data and specifications are subject to change without notice.

For additional information or questions, please contact: Nuvoton Technology Corporation.

www.nuvoton.com

1 功能介绍

1.1 简介

此示例代码演示如何实现软件DES（数据加密标准）以及DES加密/解密的工作原理。

1.2 原理

DES是一种使用64位文本块的对称加密系统。它实现了16轮加密功能和密钥生成器，并为加密功能生成48位密钥，如图1-1所示：

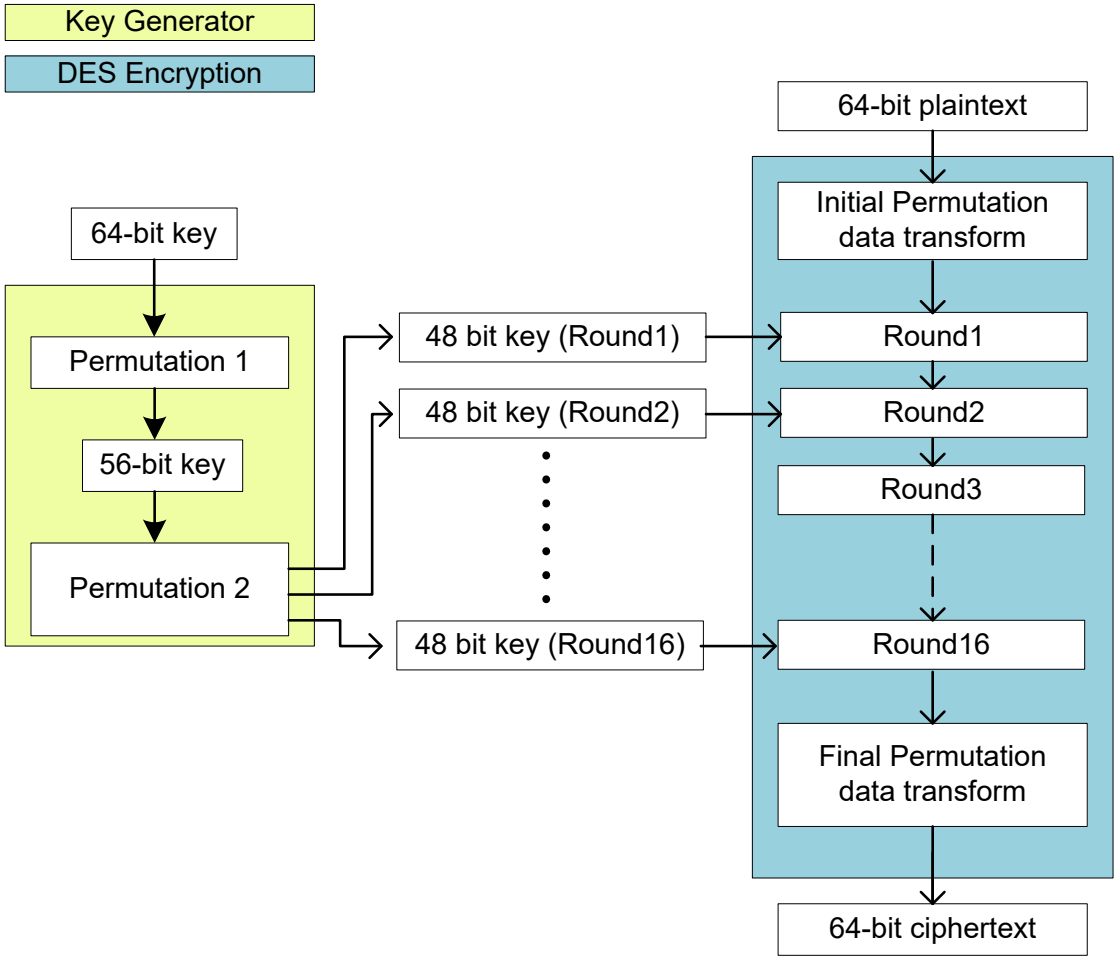

图 1-1 DES 加密模块和密钥生成器

密钥生成器使用64位密钥作为输入，输出则是16个用于DES加密的48位密钥。 DES加密函数将64位明文和来自密钥生成器的16个密钥作为输入。通过初始置换将64位明文转换为另一个64位数据，然后进入16轮加密过程。最后，执行最终排列，最后输出64位密文。而DES解密函数

则是以64位的密文为输入，同样经过16轮的解密运算，最后输出64位的明文。

1.3 执行结果

执行结果可以在 UART 上输出，鲍率 115200，如图 1-2 所示：

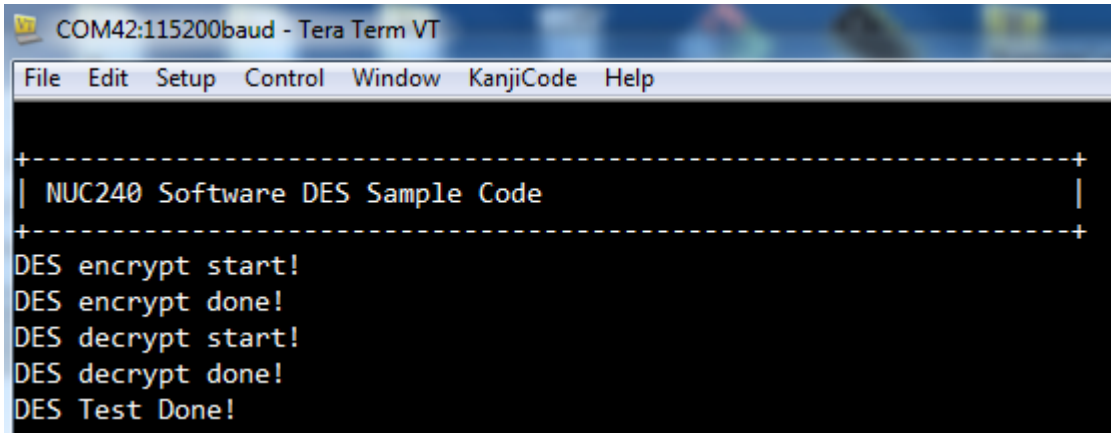

图 1-2 UART 上打印执行结果

2 代码介绍

下方的函式为如何为 DES 生成 48 位密钥：

```
/*---------------------------------------------------------------------------*/
/*  Set DES Private Key Function                                             */
/*---------------------------------------------------------------------------*/
void SetKey(char acMyKey[8])
{
    int i;
    static uint8_t au8Key_bit[64] = { 0 };
    static uint8_t *pu8Key_bit_L, *pucKey_bit_R;

    pu8Key_bit_L = &au8Key_bit[0];
    pucKey_bit_R = &au8Key_bit[28];
    ByteToBit(au8Key_bit, acMyKey, 64);

    /* Key transform: 64 bit --> 56 bit */
    TableReplace(au8Key_bit, au8Key_bit, s_acPC1Table, 56);

    /* Generate keys for 16 round DES */
    for (i = 0; i<16; i++)
    {
        /* DES rotation of left 28 bits */
        LoopBit(pu8Key_bit_L, s_acMoveTable[i], 28);

        /* DES rotation of right 28 bits */
        LoopBit(pucKey_bit_R, s_acMoveTable[i], 28);

        /* Key transform: 56 bit --> 48 bit */
        TableReplace(s_au8SubKey[i], au8Key_bit, s_acPC2Table, 48);
    }
}
```

下方的函式为 DES 加密过程：

```
/*---------------------------------------------------------------------------*/
/*  DES Encrypt Function                                                     */
/*---------------------------------------------------------------------------*/
void RunDesEncrypt(char acg_acMyMessage[8], char acHexMssage[16])
{
```

```
    int i;
    static uint8_t au8Message_bit[64] = { 0 };
    static uint8_t *Message_bit_L = &au8Message_bit[0], *Message_bit_R =
&au8Message_bit[32];
    static uint8_t au8Temp[32] = { 0 };

    /* Convert byte message to bit */
    ByteToBit(au8Message_bit, acg_acMyMessage, 64);

    /* Data transform by IP Table*/
    TableReplace(au8Message_bit, au8Message_bit, g_acIPTable, 64);

    /* DES 16-round encryption */
    for (i = 0; i<16; i++)
    {
        BitCopy(au8Temp, Message_bit_R, 32);
        FChange(Message_bit_R, s_au8SubKey[i]);
        Xor(Message_bit_R, Message_bit_L, 32);
        BitCopy(Message_bit_L, au8Temp, 32);
    }

    /* Data transform by IPR Table*/
    TableReplace(au8Message_bit, au8Message_bit, g_acIPRTable, 64);

    /* Convert bit message to hex */
    BitToHex(acHexMssage, au8Message_bit, 64);
}
```

下方的函式为 DES 解密过程：

```
/*---------------------------------------------------------------------------*/
/*  DES Decrypt Function                                                     */
/*---------------------------------------------------------------------------*/
void RunDesDecrypt(char acg_acMyMessage[8], char acHexMessage[16])
{
    int i = 0;
    static uint8_t au8Message_bit[64] = { 0 };
    static uint8_t * Message_bit_L = &au8Message_bit[0], *Message_bit_R =
&au8Message_bit[32];
    static uint8_t au8Temp[32] = { 0 };

    /* Convert hex message to bit */
    HexToBit(au8Message_bit, acHexMessage, 64);
```

```
    /* Data transform by IP Table*/
    TableReplace(au8Message_bit, au8Message_bit, g_acIPTable, 64);

    /* DES 16-round decryption */
    for (i = 15; i >= 0; i--)
    {
        BitCopy(au8Temp, Message_bit_L, 32);
        FChange(Message_bit_L, s_au8SubKey[i]);
        Xor(Message_bit_L, Message_bit_R, 32);
        BitCopy(Message_bit_R, au8Temp, 32);
    }

    /* Data transform by IPR Table*/
    TableReplace(au8Message_bit, au8Message_bit, g_acIPRTable, 64);

    /* Convert bit message to byte */
    BitToByte(acg_acMyMessage, au8Message_bit, 64);

}
```

3 软件与硬件环境

- **软件环境**
  - BSP 版本
    - NUC230/240 Series BSP CMSIS v3.01.002
  - IDE 版本
    - Keil uVersion 5.28
- **硬件环境**
  - 电路组件
    - NuTiny–EVB–NUC240–LQFP100 V1.0
  - 示意图
    - 将 UART TX（PB.1）pin 脚连接到 PC UART RX，以显示示例代码的执行结果于 PC 上。

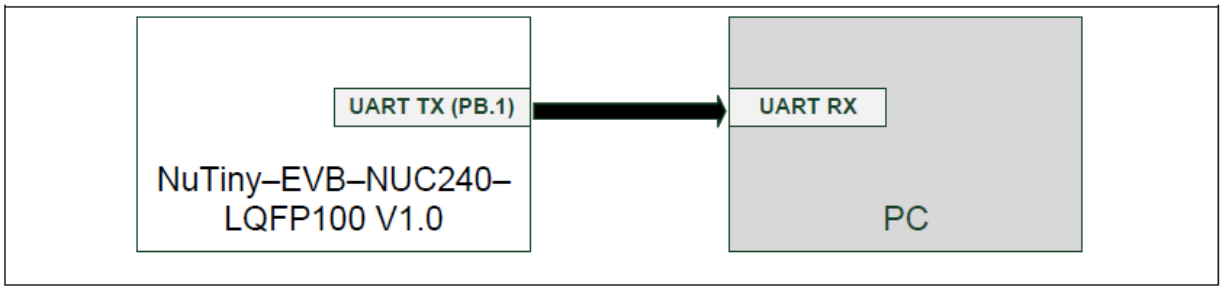

图 3-1 NUC240 UART TX 和 PC UART RX 连接

4 目录信息

- EC_NUC240_Software_DES_V1.00
  - Library — Sample code header and source files
    - CMSIS — Cortex® Microcontroller Software Interface Standard (CMSIS) by Arm® Corp.
    - Device — CMSIS compliant device header file
    - StdDriver — All peripheral driver header and source files
  - SampleCode
    - ExampleCode — Source file of example code

5 如何执行范例程序

1. 根据目录信息章节进入 ExampleCode 路径中的 KEIL 文件夹，双击 Software_DES.uvproj。
2. 进入编译模式接口
   a. 编译
   b. 下载代码至内存
   c. 进入 / 离开除错模式
3. 进入除错模式接口
   a. 执行代码

6 修订纪录

Date	Revision	Description
Sep. 9, 2019	1.00	1. 初始发布.

Important Notice

Nuvoton Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, "Insecure Usage".

Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, the control or operation of dynamic, brake or safety systems designed for vehicular use, traffic signal instruments, all types of safety devices, and other applications intended to support or sustain life.

All Insecure Usage shall be made at customer's risk, and in the event that third parties lay claims to Nuvoton as a result of customer's Insecure Usage, customer shall indemnify the damages and liabilities thus incurred by Nuvoton.

Please note that all data and specifications are subject to change without notice.
All the trademarks of products and companies mentioned in this datasheet belong to their respective owners.