軟體實作 DES

NuMicro® 32 位系列微控制器範例代碼介紹

文件資訊

代碼簡述	用軟體實作 Data Encryption Standard 算法
BSP 版本	NUC230/240 Series BSP v3.01.002
開發平台	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 功能介紹

1.1 簡介

此示例代碼演示如何實現軟件DES（數據加密標準）以及DES加密/解密的工作原理。

1.2 原理

DES是一種使用64位文本塊的對稱加密系統。它實現了16輪加密功能和密鑰生成器，並為加密功能生成48位密鑰，如圖1-1所示：

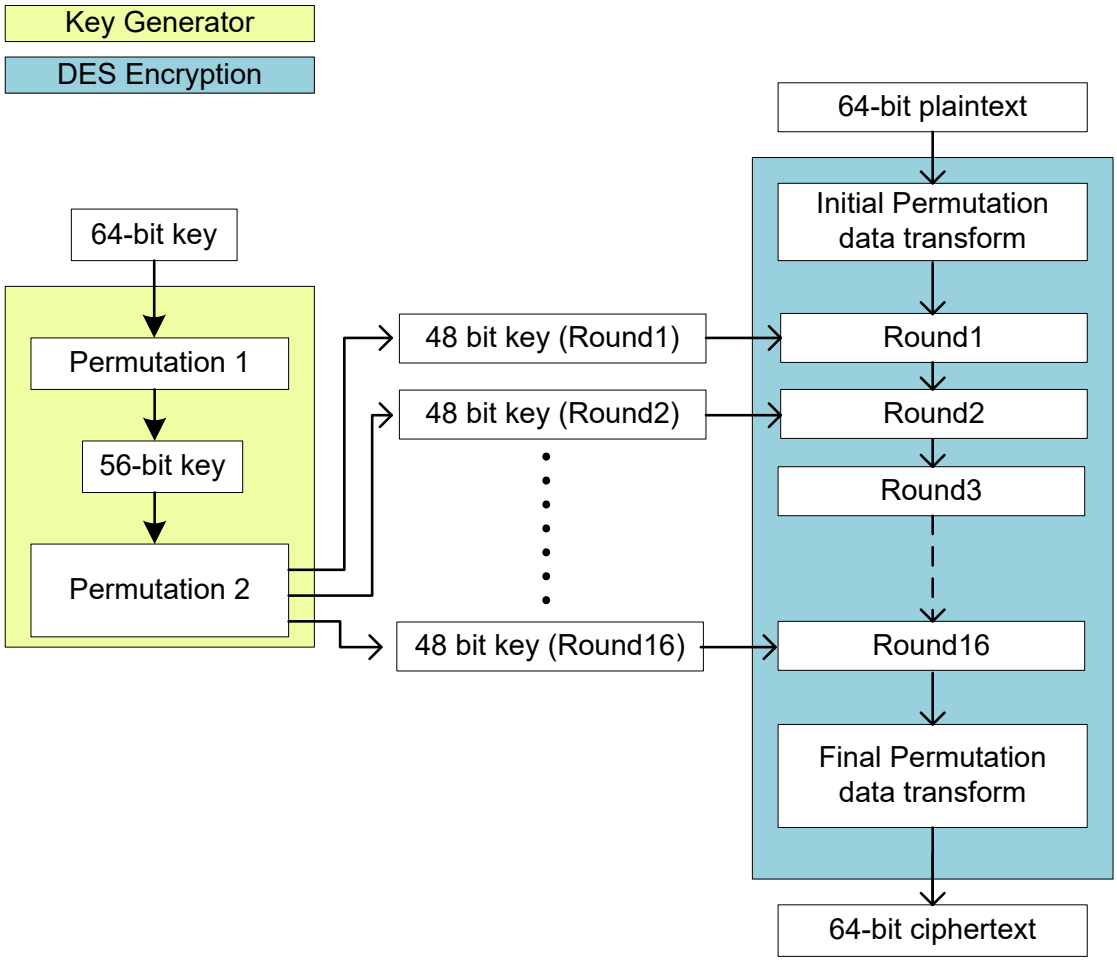

圖 1-1 DES 加密模塊和密鑰生成器

密鑰生成器使用64位密鑰作為輸入，輸出則是16個用於DES加密的48位密鑰。DES加密函數將64位明文和來自密鑰生成器的16個密鑰作為輸入。通過初始置換將64位明文轉換為另一個64位數據，然後進入16輪加密過程。最後，執行最終排列，最後輸出64位密文。而DES解密函數則

是以64位的密文為輸入，同樣經過16輪的解密運算，最後輸出64位的明文。

1.3 執行結果

執行結果可以在UART上輸出，鮑率115200，如圖1-2所示：

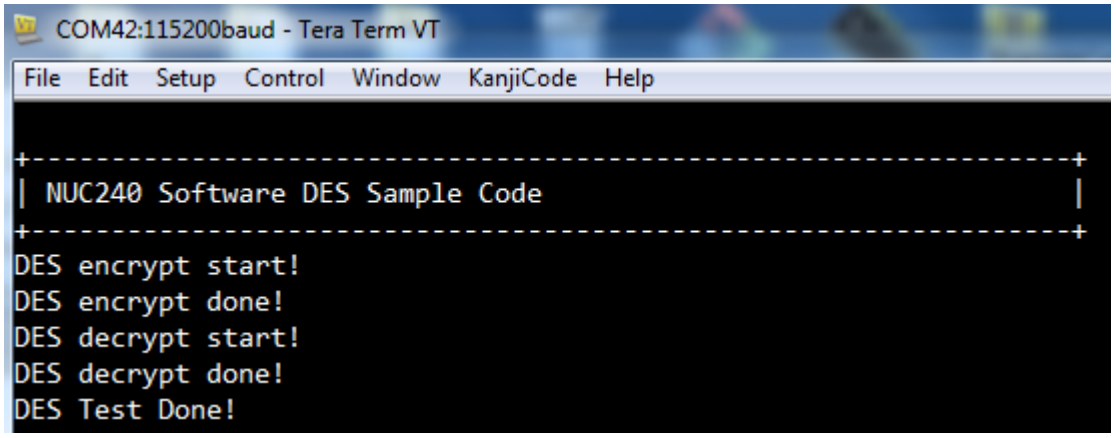

圖 1-2 UART 上打印執行結果

2 代碼介紹

下方的函式為如何為 DES 生成 48 位密鑰：

```
/*---------------------------------------------------------------------------*/
/*  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);
    }
}
```

下方的函式為 DES 加密過程：

```
/*---------------------------------------------------------------------------*/
/*  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);
}
```

下方的函式為 DES 解密過程：

```
/*---------------------------------------------------------------------------*/
/*  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 軟體與硬體環境

- **軟體環境**
  - BSP 版本
    - NUC230/240 Series BSP CMSIS v3.01.002
  - IDE 版本
    - Keil uVersion 5.28
- **硬體環境**
  - 電路元件
    - NuTiny–EVB–NUC240–LQFP100 V1.0
  - 示意圖
    - 將 UART TX（PB.1）pin 腳連接到 PC UART RX，以顯示示例代碼的執行結果於 PC 上。

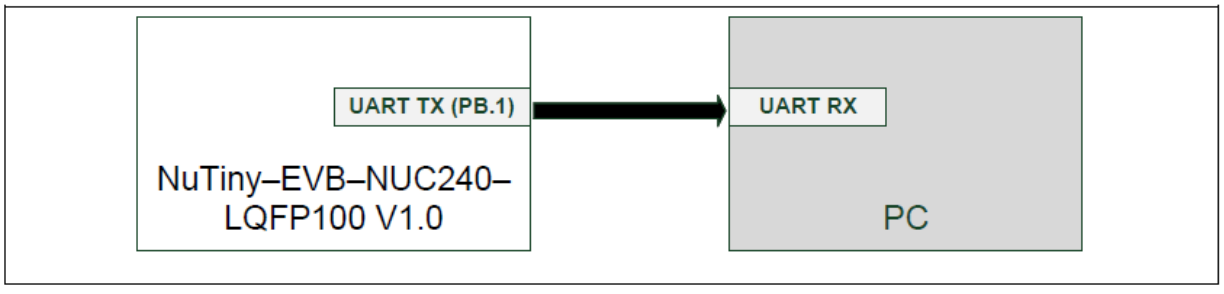

圖 3-1 NUC240 UART TX 和 PC UART RX 連接

4 目錄資訊

- 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 如何執行範例程式

1. 根據目錄資訊章節進入 ExampleCode 路徑中的 KEIL 資料夾，雙擊 Software_DES.uvproj。
2. 進入編譯模式介面
   a. 編譯
   b. 下載代碼至記憶體
   c. 進入 / 離開除錯模式
3. 進入除錯模式介面
   a. 執行代碼

6 修訂紀錄

Date	Revision	Description
Sep. 9, 2019	1.00	1. 初始發布.

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.