

RX Family

R20AN0035EJ0100

Rev.1.00

M3S-DES-LIB: DES Library

Dec 09, 2010

Introduction

This document explains the usage of the DES crypto library along with a sample program.

Target Device

RX family

Contents

1. Introduction.....	2
2. Library type definitions	3
3. Library functions	4
4. Sample program.....	7
5. Library characteristic	8
Website and Support	9
Revision Record	10
General Precautions in the Handling of MPU/MCU Products	11

1. Introduction

The DES (Data Encryption Standard) Crypto Library for RX series (hereinafter referred to as the DES Crypto Library) is the software library incorporated in the RX family and includes the data encryption/decryption functions that use the DES encryption technology. This explains how to use the DES Crypto Library.

Reference Documents:

The following documents are for reference on the specifications and standards related to the DES Crypto Library.

- FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES)
- NIST SP-800 38A, Recommendation for Block Cipher Modes of Operation

1.1 DES algorithm

The DES algorithm is a symmetric block cipher that can encrypt and decrypt information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. In the DES algorithm, 56-bit cipher key is used to generate a 64-bit ciphertext. A different key called round key(128byte data) is used in each round, and is generated from the given 64-bit key of which 56 bits are randomly generated and used directly by the algorithm. This is called key schedule. Key schedule has to be performed at least once. When the same key is used for encryption and decryption, key schedule does not have to be performed again.

1.2 Block Cipher Modes of Operation

The NIST SP 800-38A includes several modes of block cipher to generate ciphertext blocks by encrypting plaintext blocks. The DES Crypto Library supports only ECB mode.

- ECB (Electronic CodeBook) Mode

The ciphertext is created by simply encrypting each block of plaintext with the cipher key to form the corresponding block of ciphertext.

- CBC (Cipher Block Chaining) Mode

Each block of plaintext to be encrypted is XORed with the previous block of ciphertext. The result is then encrypted with the cipher key to create the corresponding block of ciphertext. Since there is no previous block of ciphertext for the first block, an initialization vector (ivec) is used in place of the previous block of ciphertext block.

2. Library type definitions

This section gives the details about the type definitions used in the library.

Datatype	Typedef
unsigned char	uint8_t
unsigned short	uint16_t
unsigned long	uint32_t
signed char	int8_t
signed short	int16_t
signed long	int32_t

3. Library functions

3.1 Key Schedule Function

Prototype

```
void R_Des_Keysch(uint8_t *key, uint32_t *ekey);
```

Explanation

This function generate round key.

The application specifies address of 64bit key data to the first argument "key".

And the application specifies address to store round key to the second argument "ekey".

This function needs must allocate more than 128 byte area for ekey.

Arguments

Argument	Type	Explanation
key	uint8_t*	A storage address of the key to 64Bit value
ekey	uint32_t*	The storage address of the value of the round key to 128Byte

Return value

Type	Explanation
void	None

Remark

When an invalid pointer (ex. NULL) is passed as a parameter, the function's behavior is undefined. 64bit DES key data has parity bit in [bit7, bit15, bit23, bit31, bit39, bit47, bit55, bit63]. But this function does not check these parity bits.

3.2 Encryption Function (ECB mode)

Prototype

```
void R_Des_Ecbenc(uint8_t *pdat, uint8_t *cdat, uint32_t *ekey, uint32_t
block);
```

Explanation

This function encrypts the data with ECB mode.

The application specifies address to encrypt data area to first argument "pdat".

The function stores the encrypted data to second argument "cdat".

The application specifies address of round key data to third argument "ekey".

The application specifies block size to fourth argument "block".

Arguments

Argument	Type	Explanation
pdat	uint8_t*	Original data address to code
cdat	uint8_t*	Address to code of the result that I coded
ekey	uint32_t*	Round key
block	uint32_t	Quantity of data block(unit:1block = 8byte)

Return value

Type	Explanation
void	None

Remark

When an invalid pointer (ex. NULL) is passed as a parameter, the function's behavior is undefined.

When original data area and encrypted data area are overlapped, the function's behavior is undefined.

In case excluded message area and hash area are same pointer.

3.3 Decryption Function (ECB mode)

Prototype

```
void R_Des_Ecbdec(uint8_t *cdat, uint8_t *pdat, uint32_t *ekey, uint32_t
block);
```

Explanation

This function decrypts the data with ECB mode.

The application specifies address to decrypt data area to first argument "cdat".

The function stores the decrypted data to second argument "pdat".

The application specifies address of round key data to third argument "ekey".

The application specifies block size to fourth argument "block".

Arguments

Argument	Type	Explanation
cdat	uint8_t*	An address to store away a decoded result
pdat	uint8_t*	The address of coded data
ekey	uint32_t*	Round key
block	uint32_t	Quantity of data block(unit:1block = 8byte)

Return value

Type	Explanation
void	None

Remark

When an invalid pointer (ex. NULL) is passed as a parameter, the function's behavior is undefined.

When encrypt data area and decoded data area are overlapped, the function's behavior is undefined.

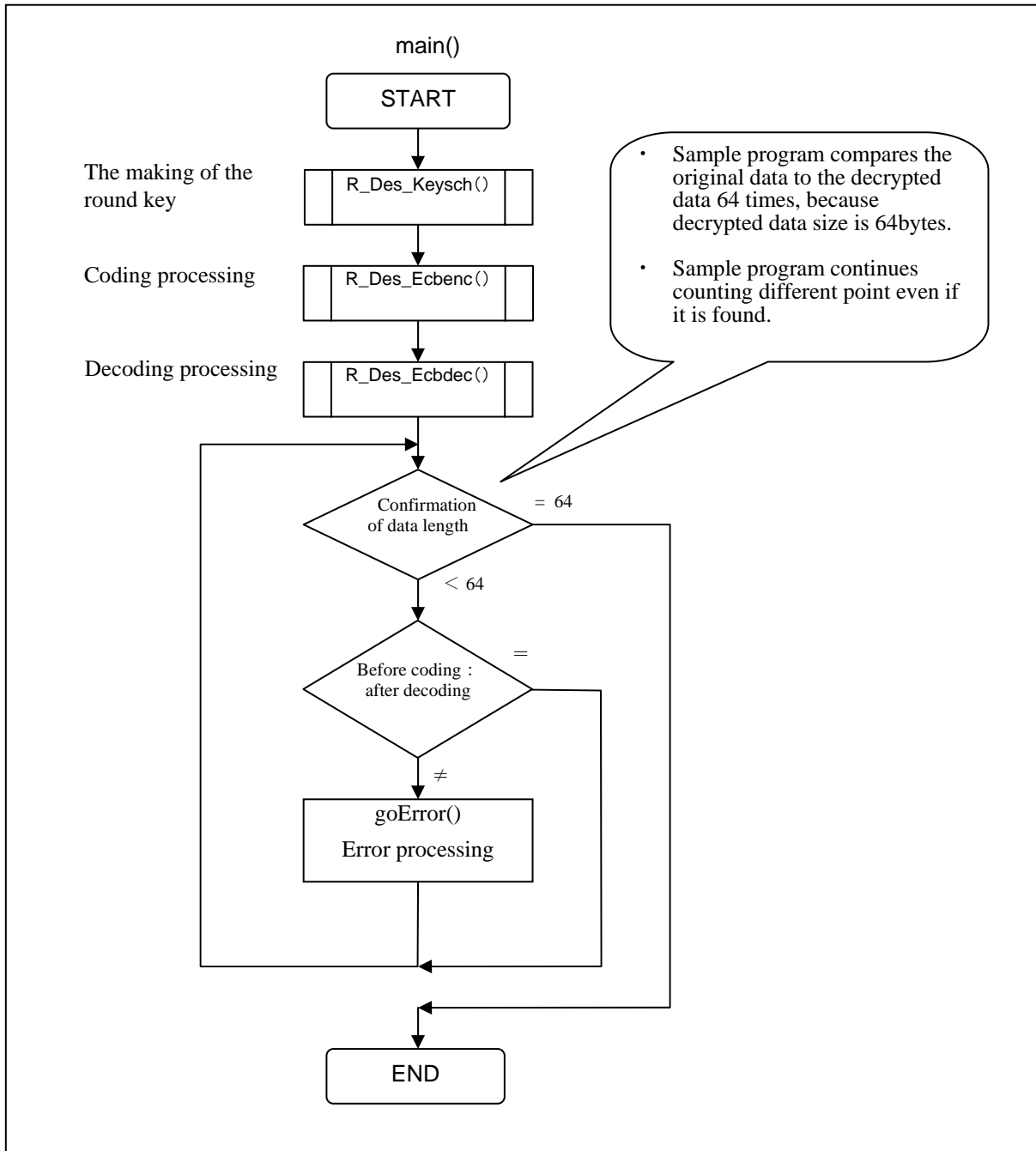
In case excluded message area and hash area are same pointer.

4. Sample program

This section explains the sample program for DES encryption and decryption.

4.1 Outline

The sample program confirms that a decryption result of a ciphertext equals to the original plaintext of the ciphertext which the sample program decrypted.



5. Library characteristic

5.1 Occupied memory size

Microcomputer	ROM	RAM	Stack		
			R_Des_Keysch	R_Des_Ecbenc	R_Des_Ecbdec
RX600	1,600 Byte	160 Byte	40 Byte	60 Byte	60 Byte

5.2 Encryption/Decryption processing speed

Microcomputer	processing time(*)		
	R_Des_Keysch	R_Des_Ecbenc	R_Des_Ecbdec
RX600	1227 cycles	993 cycles x N + 93 cycles	1,009 cycles x N + 92 cycles

* N = number of block; 1 block = 8 byte

Website and Support

Renesas Electronics Website

<http://www.renesas.com/>

Inquiries

<http://www.renesas.com/inquiry>

All trademarks and registered trademarks are the property of their respective owners.

Revision Record

Rev.	Date	Description	
		Page	Summary
1.00	Dec.09.10	—	First edition issued

General Precautions in the Handling of MPU/MCU Products

The following usage notes are applicable to all MPU/MCU products from Renesas. For detailed usage notes on the products covered by this manual, refer to the relevant sections of the manual. If the descriptions under General Precautions in the Handling of MPU/MCU Products and in the body of the manual differ from each other, the description in the body of the manual takes precedence.

1. Handling of Unused Pins

Handle unused pins in accord with the directions given under Handling of Unused Pins in the manual.

- The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible. Unused pins should be handled as described under Handling of Unused Pins in the manual.

2. Processing at Power-on

The state of the product is undefined at the moment when power is supplied.

- The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the moment when power is supplied.

In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the moment when power is supplied until the reset process is completed.

In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the moment when power is supplied until the power reaches the level at which resetting has been specified.

3. Prohibition of Access to Reserved Addresses

Access to reserved addresses is prohibited.

- The reserved addresses are provided for the possible future expansion of functions. Do not access these addresses; the correct operation of LSI is not guaranteed if they are accessed.

4. Clock Signals

After applying a reset, only release the reset line after the operating clock signal has become stable.

When switching the clock signal during program execution, wait until the target clock signal has stabilized.

- When the clock signal is generated with an external resonator (or from an external oscillator) during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Moreover, when switching to a clock signal produced with an external resonator (or by an external oscillator) while program execution is in progress, wait until the target clock signal is stable.

5. Differences between Products

Before changing from one product to another, i.e. to one with a different type number, confirm that the change will not lead to problems.

- The characteristics of MPU/MCU in the same group but having different type numbers may differ because of the differences in internal memory capacity and layout pattern. When changing to products of different type numbers, implement a system-evaluation test for each of the products.

Notice

- All information included in this document is current as of the date this document is issued. Such information, however, is subject to change without any prior notice. Before purchasing or using any Renesas Electronics products listed herein, please confirm the latest product information with a Renesas Electronics sales office. Also, please pay regular and careful attention to additional and different information to be disclosed by Renesas Electronics such as that disclosed through our website.
- Renesas Electronics does not assume any liability for infringement of patents, copyrights, or other intellectual property rights of third parties by or arising from the use of Renesas Electronics products or technical information described in this document. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
- You should not alter, modify, copy, or otherwise misappropriate any Renesas Electronics product, whether in whole or in part.
- Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation of these circuits, software, and information in the design of your equipment. Renesas Electronics assumes no responsibility for any losses incurred by you or third parties arising from the use of these circuits, software, or information.
- When exporting the products or technology described in this document, you should comply with the applicable export control laws and regulations and follow the procedures required by such laws and regulations. You should not use Renesas Electronics products or the technology described in this document for any purpose relating to military applications or use by the military, including but not limited to the development of weapons of mass destruction. Renesas Electronics products and technology may not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations.
- Renesas Electronics has used reasonable care in preparing the information included in this document, but Renesas Electronics does not warrant that such information is error free. Renesas Electronics assumes no liability whatsoever for any damages incurred by you resulting from errors in or omissions from the information included herein.
- Renesas Electronics products are classified according to the following three quality grades: "Standard", "High Quality", and "Specific". The recommended applications for each Renesas Electronics product depends on the product's quality grade, as indicated below. You must check the quality grade of each Renesas Electronics product before using it in a particular application. You may not use any Renesas Electronics product for any application categorized as "Specific" without the prior written consent of Renesas Electronics. Further, you may not use any Renesas Electronics product for any application for which it is not intended without the prior written consent of Renesas Electronics. Renesas Electronics shall not be in any way liable for any damages or losses incurred by you or third parties arising from the use of any Renesas Electronics product for an application categorized as "Specific" or for which the product is not intended where you have failed to obtain the prior written consent of Renesas Electronics. The quality grade of each Renesas Electronics product is "Standard" unless otherwise expressly specified in a Renesas Electronics data sheets or data books, etc.
"Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; and industrial robots.
"High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control systems; anti-disaster systems; anti-crime systems; safety equipment; and medical equipment not specifically designed for life support.
"Specific": Aircraft; aerospace equipment; submersible repeaters; nuclear reactor control systems; medical equipment or systems for life support (e.g. artificial life support devices or systems), surgical implantations, or healthcare intervention (e.g. excision, etc.), and any other applications or purposes that pose a direct threat to human life.
- You should use the Renesas Electronics products described in this document within the range specified by Renesas Electronics, especially with respect to the maximum rating, operating supply voltage range, movement power voltage range, heat radiation characteristics, installation and other product characteristics. Renesas Electronics shall have no liability for malfunctions or damages arising out of the use of Renesas Electronics products beyond such specified ranges.
- Although Renesas Electronics endeavors to improve the quality and reliability of its products, semiconductor products have specific characteristics such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Further, Renesas Electronics products are not subject to radiation resistance design. Please be sure to implement safety measures to guard them against the possibility of physical injury, and injury or damage caused by fire in the event of the failure of a Renesas Electronics product, such as safety design for hardware and software including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult, please evaluate the safety of the final products or system manufactured by you.
- Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. Please use Renesas Electronics products in compliance with all applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive. Renesas Electronics assumes no liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
- This document may not be reproduced or duplicated, in any form, in whole or in part, without prior written consent of Renesas Electronics.
- Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products, or if you have any other inquiries.
(Note 1) "Renesas Electronics" as used in this document means Renesas Electronics Corporation and also includes its majority-owned subsidiaries.
(Note 2) "Renesas Electronics product(s)" means any product developed or manufactured by or for Renesas Electronics.



SALES OFFICES

Renesas Electronics Corporation

<http://www.renesas.com>

Refer to "<http://www.renesas.com/>" for the latest and detailed information.

Renesas Electronics America Inc.

2880 Scott Boulevard Santa Clara, CA 95050-2554, U.S.A.
Tel: +1-408-588-6000, Fax: +1-408-588-6130

Renesas Electronics Canada Limited

1101 Nicholson Road, Newmarket, Ontario L3Y 9C3, Canada
Tel: +1-905-898-5441, Fax: +1-905-898-3220

Renesas Electronics Europe Limited

Dukes Meadow, Millboard Road, Bourne End, Buckinghamshire, SL8 5FH, U.K.
Tel: +44-1628-585-100, Fax: +44-1628-585-900

Renesas Electronics Europe GmbH

Arcadiastrasse 10, 40472 Düsseldorf, Germany
Tel: +49-211-6503-0, Fax: +49-211-6503-1327

Renesas Electronics (China) Co., Ltd.

7th Floor, Quantum Plaza, No.27 ZhiChunLu Haidian District, Beijing 100083, P.R.China
Tel: +86-10-8235-1155, Fax: +86-10-8235-7679

Renesas Electronics (Shanghai) Co., Ltd.

Unit 204, 205, AZIA Center, No.1233 Lujiazui Ring Rd., Pudong District, Shanghai 200120, China
Tel: +86-21-5877-1818, Fax: +86-21-6887-7858 / -7898

Renesas Electronics Hong Kong Limited

Unit 1601-1613, 16/F., Tower 2, Grand Century Place, 193 Prince Edward Road West, Mongkok, Kowloon, Hong Kong
Tel: +852-2886-9318, Fax: +852-2886-9022/9044

Renesas Electronics Taiwan Co., Ltd.

7F, No. 363 Fu Shing North Road Taipei, Taiwan, R.O.C.
Tel: +886-2-8175-9600, Fax: +886-2-8175-9670

Renesas Electronics Singapore Pte. Ltd.

1 HarbourFront Avenue, #06-10, Keppel Bay Tower, Singapore 098632
Tel: +65-6213-0200, Fax: +65-6278-8001

Renesas Electronics Malaysia Sdn.Bhd.

Unit 906, Block B, Menara Amcorp, Amcorp Trade Centre, No. 18, Jln Persiaran Barat, 46050 Petaling Jaya, Selangor Darul Ehsan, Malaysia
Tel: +60-3-7955-9390, Fax: +60-3-7955-9510

Renesas Electronics Korea Co., Ltd.

11F., Samik Lavied' or Bldg., 720-2 Yeoksam-Dong, Kangnam-Ku, Seoul 135-080, Korea
Tel: +82-2-558-3737, Fax: +82-2-558-5141