NEC

Application Note

78K0R

16-Bit Single-Chip Microcontrollers

DES Encryption/Decryption

Document No. U19669EE1V0AN00
Date Published August 2009

DISCLAIMER

The related documents in this application note may include preliminary versions. However, preliminary versions may not have been marked as such.

The information in this application note is current as of its date of publication. The information is subject to change without notice. For actual design-in, refer to the latest publications of NEC's data sheets or data books, etc., for the most up-to-date specifications of PRODUCT(S). Not all PRODUCT(S) and/or types are available in every country. Please check with an NEC sales representative for availability and additional information.

No part of this application note may be copied or reproduced in any form or by any means without prior written consent of NEC. NEC assumes no responsibility for any errors that may appear in this application note. NEC 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 PRODUCT(S) listed in this application note or any other liability arising from the use of such PRODUCT(S).

No license, express, implied or otherwise, is granted under any patents, copyrights or other intellectual property rights of NEC or others. Descriptions of circuits, software and other related information in this application note are provided for illustrative purposes of PRODUCT(S) operation and/or application examples only. The incorporation of these circuits, software and information in the design of customer's equipment shall be done under the full responsibility of customer. NEC assumes no responsibility for any losses incurred by customers or third parties arising from the use of these circuits, software and information.

While wherever feasible, NEC endeavors to enhance the quality, reliability and safe operation of PRODUCT(S) the customer agrees and acknowledges that the possibility of defects and/or erroneous thereof cannot be eliminated entirely. To minimize risks of damage to property or injury (including death) to persons arising from defects and/or errors in PRODUCT(S) the customer must incorporate sufficient safety measures in their design, such as redundancy, fire-containment and anti-failure features.

The customer agrees to indemnify NEC against and hold NEC harmless from any and all consequences of any and all claims, suits, actions or demands asserted against NEC made by a third party for damages caused by one or more of the items listed in the enclosed table of content of this application note for PRODUCT(S) supplied after the date of publication.

PRODUCT(S) are classified into the following three quality grades: "Standard", "Special" and "Specific". The "Specific" quality grade applies only to PRODUCT(S) developed based on a customer-designated "quality assurance program" for a specific application. The recommended applications of PRODUCT(S) depend on its quality grade, as indicated below. Customers must check the quality grade of each PRODUCT(S) before using it in a particular application.

- "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
- "Special": 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, life support systems and medical equipment for life support etc.

The quality grade of PRODUCT(S) is "Standard" unless otherwise expressly specified in NEC data sheets or data books, etc. If customers wish to use PRODUCT(S) in applications not intended by NEC, they must contact NEC sales representative in advance to determine NEC's willingness to support a given application.

If the supplied goods/information are subject to Japanese, German, European and/or North American export controls, the customer shall comply with the relevant export control regulations in the event that the goods are exported and/or re-exported. If deliveries are exported without payment of duty at the request of the customer, the customer accepts liability for any subsequent customs administration claims with respect to NEC.

Notes: (1) "**NEC**" as used in this statement means NEC Electronics Corporation and also includes its direct or indirect owned or controlled subsidiaries.

(2) "**PRODUCT(S)**" means any product developed or manufactured by or for NEC (as defined above).

Table of Contents

78K0R

Chapter 1 Supporting Data Security

NEC Electronics Europe (GmbH) has coded the **Data Encryption Standard** (**DES**) to our 16-bit 78K0R microcontroller, with a view to providing unrestricted DES middleware libraries free-of-charge to designers.

There are three main components included in the library:
- Source code of the encryption, decryption routines.
- Associated header file for the above.
- Test routines to verify the result and the execution speed of the routines provided.

The software supports encryption key lengths of 64-bits and can be used with any 78K0R/Kx3-L ,/IX3 ,/LX3 or /FX3 family microcontroller.

Implementing the library is very straightforward, following this simple process:
- Call a function that initializes the keys that will be used to encrypt or decrypt the messages; you just need to pass the key (64-bits) to the library function.
  i.ex:

  subkey_crypt(key,encrypt);

  key is the pointer to the 64-bit key which shall be used for en-/decrytion
  encrypt is an enumerator which controls the generation of the needed subkeys

- Call a function to encrypt/decrypt a 64-bit message; the result is the de-/encrypted 64-bit message.
  i.ex:
  encrypt_decrypt((uint8 *)(pln));
  pln is the pointer to the array/string which shall be en-/decrypted.
  the result is returned in an array called gData.

Two test functions are also provided by NEC Electronics. These functions, called test_encrypt / test_decrypt, perform three en-/de-cryptions with a given key. Comparison can be done by checking the output data with the reference values given in the comments of the source code.
(The source code is attached to the pdf).

Details on this validation method can be found on the Internet at
http://en.wikipedia.org/wiki/Data_Encryption_Standard.
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
http://people.eku.edu/styere/Encrypt/JS-DES.html

It goes without saying that responsibility for the actual implementation lies with the user of the middleware.

In terms of resource required, our middleware requires 3315bytes of code memory, 698 bytes of data memory and 576 bytes of constant memory, based on its usage in a K0R 16-bit microcontroller.

It should be noted that whilst developed with a 16-bit microcontroller in mind, given the availability of ‘C’ source code in NEC Electronics’ library, it would be practical to easily port the code to a 32-bit or even an 8-bit microcontroller, although the required response time should be considered as the CPU clock speed of the selected NEC Electronics microcontroller decreases.

Further details are available by contacting NEC Electronics at www.eu.necel.com.

Chapter 2 Revision History

Item	Date published	Document No.	Comment
1	August 24, 2009	U19669EE1V0AN00	1st Release