

ALGORITHM REGISTER ENTRY

- a) ISO Entry Name {iso standard 9979 encrip (14)}
- b) Name of Algorithm ENCRiP
- c) Intended Range of Application
1. Confidentiality
 2. Hash Function - as detailed in ISO 10118-2
 3. Authentication - as detailed in ISO 9798
 4. Data Integrity - as detailed in ISO 9797
- d) Cryptographic Interface Parameters
1. Input size 64 bits
 2. Output size 64 bits
 3. Key length: 64 bits
 4. Round number positive integer
- e) Test Data
- | | |
|--------------|--------------------------------------|
| ROUND NUMBER | 8 |
| KEY | (0000 0000 0000 0000) _{hex} |
| INPUT DATA | (0000 0000 0000 0000) _{hex} |
| OUTPUT DATA | (ad42 9039 cbad 6d03) _{hex} |
|
 | |
| KEY | (0123 4567 89ab cdef) _{hex} |
| INPUT DATA | (0000 0000 0000 0000) _{hex} |
| OUTPUT DATA | (82cc cb37 3104 36fe) _{hex} |
|
 | |
| KEY | (0000 0000 0000 0000) _{hex} |
| INPUT DATA | (0123 4567 89ab cdef) _{hex} |
| OUTPUT DATA | (d927 6be7 9a3f fe06) _{hex} |
|
 | |
| KEY | (0123 4567 89ab cdef) _{hex} |
| INPUT DATA | (0123 4567 89ab cdef) _{hex} |
| OUTPUT DATA | (829c 489e d578 299d) _{hex} |
- f) Sponsoring Authority Information-Technology Promotion Agency,
Japan(IPA)
Shuwa-Shibakoen 3-chome Bldg., 6F,
3-1-38 Shibakoen,
Minato-ku, Tokyo 105, JAPAN
Tel:
+81-3-3437-2301
Fax:
+81-3-3437-9421
- Registration Requested by NEC Corporation
C&C Laboratories
- Contact for Information Yukiyasu TSUNOO
Assistant Manager
NEC Corporation
C&C Laboratories
System Basics Laboratory
4-1-1 Miyazaki, Miyamae-ku,
Kawasaki 216, JAPAN
Tel:
+81-44-856-2141
Fax:
+81-44-856-2235
- g) Date of submission: 1996.11.11
Date of registration 12 February 1997
- h) Whether the Subject of a National Standard: No.

- i) Patent - License Restriction A patent applied for:
1. Japan, No. 07-206372
For commercial use of ENCRiP, a license and fee is required.

j) References

k) Description of Algorithm

ENCRiP is a block cipher algorithm whose plaintext block is of 64 bits, whose ciphertext block is of 64 bits, and which uses a common key of 64 bits.

ENCRiP has an option, which is called 'round number'. The round number specifies the number of internal iteration of data randomization.

l) Modes of operation Mode of operation as defined in ISO 8372 are applicable.

m) Other information

The round number of ENCRiP should be decided from aspects of its strength and speed. The speed of ENCRiP is almost inversely proportional to its round number. On the other hand, the strength of ENCRiP increases exponentially by increasing its round number if the round number is small. However, it is not effective any longer to set too large round number because of the influence of the key length. The round number is recommended to be at least 8.