

- a) ISO Entry Name { ISO standard 9979 speam1 (17) }
- b) Proprietary Entry Name SPEAM1
- c) Intended Range of Applications
1. Confidentiality
 2. Authentication-as detailed in ISO/IEC9798-2
 3. Data Integrity - as detailed in ISO/IEC9797
 4. Hash Function-as detailed in ISO/IEC10118-2
- d) Cryptographic Interface Parameters
1. Input size - 64bits
 2. Output size - 64bits
 3. Key length - 128bits
 4. Round number-a multiple of four(not less than 8)
- e) Test Data
1. Round number - 8
 2. Key - b3a29180 f7e6d5c4 76543210 fedcba98
 3. Input data - abcdef01 23456789
 4. Output data - 79a8e064 6df7c516
- f) The identification of the Organization
- Sponsoring Authority:
 Information-Technology Promotion Agency,
 Japan(IPA)
 Shuwashibakoen 3-chome Bldg. 6F
 3-1-38 Shibakoen, Minato-ku, Tokyo 105, Japan
 Phone +81-3-3437-2301
 Fax +81-3-3437-2537

Registration requested by :
 Matsushita Electric Industrial Co., LTD.

Contact for Information:
 Atsuko Miyaji
 Multimedia Development Center
 Matsushita Electric Industrial Co., LTD.
 1006 Kadoma, Kadoma, Osaka, 571 JAPAN

Tel: +81-6-906-4874

Fax: +81-6-906-0576

E-mail: speam@isl.mei.co.jp

- g) Dates of Registration and Modification 5th December 1997
- h) Whether the Subject of No
a National Standard
- i) Patent License Restriction The following patent has been applied for:
Japan, No. 6-120942
Japan, No. 6-342258
- j) References See ISO8372 or ISO/IEC10116 for its
information on mode of operation
- k) Description of Algorithm
SPEAM 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 128
bits. SPEAM has a feature of a changeable iteration number, where an
iteration number means the number of iterations of a randomizing function.
- l) Modes of Operation Modes of Operation as defined in ISO/8372
or ISO/IEC10116 are applicable:
1. Electronic Codebook mode(ECB)
2. Cipher Block Chaining mode(CBC)
3. Cipher Feedback mode(CFB)
4. Output Feedback mode(OFB)