Application for Registration of Cryptographic Algorithm

a.) ISO entry name {iso standard 9979 cdmf (5)}

b.) Name of Algorithm

Commercial Data Masking Facility (CDMF)

c.) Intended Range of Applications

Confidentiality

d.) Cryptographic Interface Parameters

1. Input data: 64 bit block
2. Output data: 64 bit block
3. Key input: 64 bit block in a pattern of 7 key bits followed by one unused bit followed by 7 key bits followed by an unused bit. This pattern in continued through the 64th bit.

e.) Test Words

1.Clear key = X FFFFFFFFFFFFFFFF'
Cleartext = X 0123456789ABCDEF'
Ciphertext = X 12CC8EE83C686380'

2.Clear key = X 0000000000000000'
Cleartext = X 0123456789ABCDEF'
Cipfertext = X 79B1D72AD877D204'

3.Clear key = X 0123456789ABCDEF'
Cleartext = X 0123456789ABCDEF'
Ciphertext = X 7D74922D74B12E13'

f.) Sponsoring Authority

American National Standards Institute

Registeration requested by IBM

Contact for information

James Randall
IBM Corporation
1301 K Street N.W.
Washington D.C. 20005-3307
USA
Telephone: 1-202-515-5525
FAX: 1-202-515-5551

g.) Date of Submission 29 october 1994

h.) Whether the Subject of a National Standard

No

i.) Patent License Restriction Information

Patent filed by IBM - Pending

j.) References to Associated Algorithms

1.FIPS 46 - Data Encryption Standard (USA)
2.ANSI X3.92 - Data Encryption Algorithm (USA)

K.) Description of Algorithm

l.) Other Information

CDMF Algorithm Definition Details

In the following definition of the CDMF algorithm, all bits in a bit string are numbered from leftmost to rightmost as bit 1 to bit 64,
eK(X) represents DEA encryption of X using key K,
AND is the bitwise Boolean-AND operation,
XOR is the bitwise Boolean-Exclusive-OR operation,
and := represents the assignment operation.

The procedural definition of the CDMF algorithm is as follows:

1. Set parity bits.

   Zero the following bits in the input CDMF key:
   Bits 8, 16, 24, 32, 40, 48, 56, 64 of input CDMF key are set to zero.
   Call the result I1.

   This may be accomplished by the following:
   I1 := input-key AND X'FEFEFEFEFEFEFEFE'

2. One-way function.

   I2 := I1 XOR eK1(I1)
   where K1 is the fixed value X'C408B0540BA1E0AE'.

3. Selection function.

   Zero the following bits in I2:
   1,2,3,4,8,16,17,18,19,20,24,32,33,34,35,36,40,48,49,50,51,52,56,64.
   Call the result I3.

   This may be accomplished by the following:
   I3 := I2 AND X'0EFE0EFE0EFE0EFE'

4. Expansion function.

   The derived key K' := eK2(I3)
   where K2 is the constant DEA key X'EF2C041CE6382FE6'.

5. Regular DEA invocation.

   The derived key K' is used internally as the key in a DEA invocation.