ISO 9979/0009

ALGORITHM REGISTER ENTRY

a) ISO Entry Name		{iso standard 9979 multi2 (9)}
b) Name of Algorithm		MULTI2
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: Data key 64 bits System key 256 bits 4. Round number positive integer
e) Test Data	ROUND NUMBER	128
	SYSTEM KEY	all 0's for 256 bits of system key
	DATA KEY	(0123 4567 89AB CDEF) hex
	INPUT DATA	(0000 0000 0000 0001)hex
	INTERMEDIARY (4th ROUND)	(772F 558A F46A C13B)hex
	INTERMEDIARY (8th ROUND)	(696E F331 5EDF 0BFB)hex
	INTERMEDIARY (16h ROUND)	(9E89 DA58 87C0 B518)hex
	INTERMEDIARY (32th ROUND)	(3F98 2A1F 459A B023)hex
	INTERMEDIARY (64th ROUND)	(11BD C4D0 9DF3 99A8)hex
	OUTPUT DATA (128th ROUND)	(F894 4084 5E11 CF89)hex

f) Sponsoring Authority

Information-Technology Promotion Agency, Japan (IPA)
Shuwashibakoen 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

Hitachi, Ltd.
Software Development Center

Contact for Information

Hisashi Hashimoto
Senior Engineer
Hitachi, Ltd.
Software Development Center
Workstation Network Software Department
TYG 11th Bldg. 16-1 3-chome, Nakamachi

ISO 9979/0009

Atsugi-shi 243, JAPAN
Tel:
+81-462-25-9271
Fax:
+81-462-25-9395

g) Date of submission	
Date of registration	14 November 1994
h) Whether the Subject of a National Standard	No.
i) Patent - License Restriction	Two patents registered: 1. United States Patent, No. 4,982,429 2. United States Patent, No. 5,103,479 One patent applied for: 3. Japan, No. 63-103919 For commercial use of MULTI2, a license and fee is required.
j) References	See ISO 8372 or ISO/IEC 10116 for its information on modes of operation.
k) Description of Algorithm	MULTI2 is a symmetric block cipher algorithm based on the permutation - substitution calculation like DES. Since MULTI2 was published in 1989, the cryptographic strength of MULTI2 has been tested through a number of cryptanalysis attacks. It is designed to realize a high performance on 32-bit computers. For example, MULTI2 with the round number N=32 exhibits the memory - memory encryption speed of about 1 Mbps per 1 MIPS computing power. As the full specification of MULTI2 is open, it can be used for software implementation of security mechanisms in open/multivendor networks. See Appendix for detail.

l) Modes of operation

Modes of operation as defined in ISO 8372 or ISO/IEC 10116 are applicable:

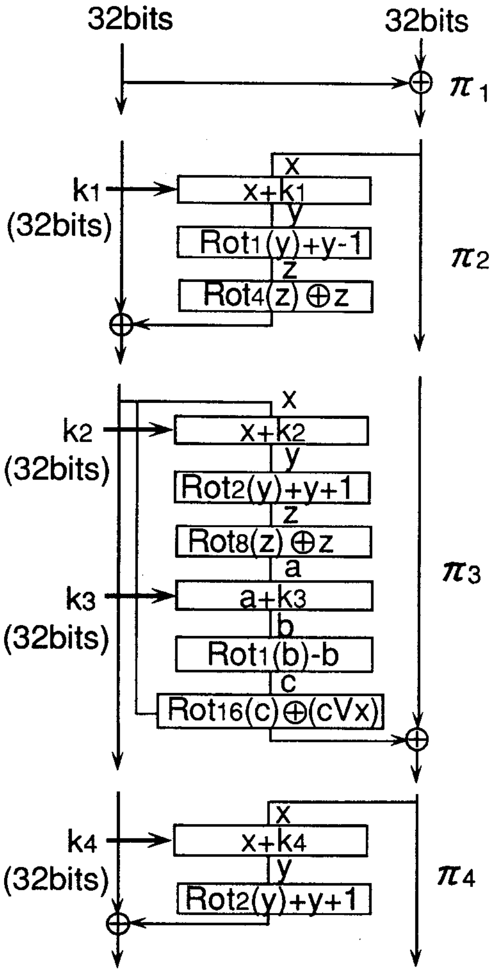
1. Electronic Codebook (ECB) Mode
2. Cipher Block Chaining (CBC) Mode
3. Cipher Feedback (CFB) Mode
4. Output Feedback (OFB) Mode

m) Other information

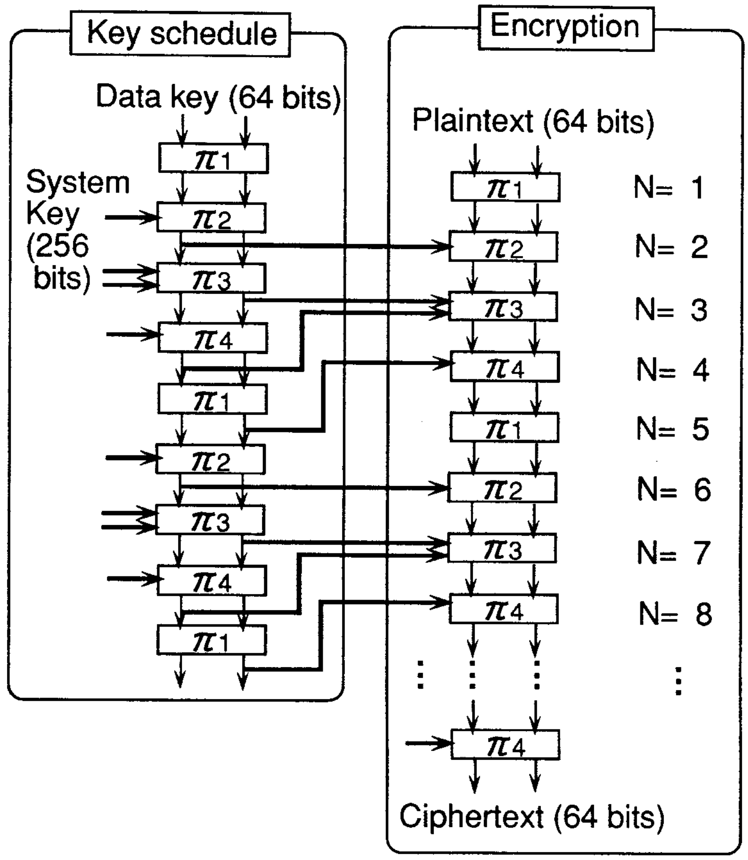
In general, it is not possible to prove that an encryption algorithm and its environment are perfectly safe. However, a comparison of cryptographic strength between two encryption algorithms may help to obtain a safety measure. It is reported that MULTI2 with the round number less than thirty-two may be broken easier than DES. However, no method has been reported which can break MULTI2 with the round number thirty-two or more. The cryptographic strength of MULTI2 algorithm becomes higher as the round number N increases. On the other hand, the speed of MULTI2 encryption is almost inversely proportional to the round number. The encryption speed of MULTI2 with the round number thirty-two is about 1 Mbps per 1 MIPS computing power. In some cases, it is recommended that a trade-off between the speed and the safety margin be examined to determine the round number of MULTI2.

APPENDIX: DETAIL OF MULTI2 ALGORITHM

Basic functions
(Involutions)



Encryption process



Symbols

⊕ : bit-wise exclusive OR, + : addition in modulus 2^{32}, - : subtraction in modulus 2^{32},

Rot_s : s bits left circular rotation, V : bit-wise logical OR, N : round number

|| : concatination of data elements,

$T_{[left]}$: the string composed of the 32 leftmost bits of the block T

$T_{[right]}$: the string composed of the 32 rightmost bits of the block T

Definition of basic functions

1. $\pi 1$

Let T be the input to $\pi 1$. Then, the output of $\pi 1$ is obtained:

$\pi 1(T)=T[left] \parallel (T[left] \oplus T[right])$

2. $\pi 2$

Let T be the input to $\pi 2$. Let k_1 be the key value. Then, the intermediates x, y and z are calculated as:

$x=T[right]$

$y=x+k_1$

$z=Rot_1(y)+y-1$

The output of $\pi 2$ is obtained:

$\pi 2_{k1}(T)=(T[left] \oplus (Rot4(z) \oplus z)) \parallel T[right]$

3. $\pi 3$

Let T be the input to $\pi 3$. Let k_2 and k_3 be the key values. Then, the intermediates x, y, z, a, b and c are calculated as:

$x=T[left]$

$y=x+k2$

$z=Rot2(y)+y+1$

$a=Rot8(z) \oplus z$

$b=a+k3$

$c=Rot_1(b)-b$

The output of $\pi 3$ is obtained:

$\pi 3_{k2,k3}(T)=T[left] \parallel (T[right] \oplus (Rot_{16}(c) \oplus (cVx)))$

4. $\pi 4$

Let T be the input to $\pi 4$. Let k_4 be the key value. Then, the intermediates x and y are calculated as:

$x=T[right]$

$y=x+k_4$

The output of $\pi 4$ is obtained:

$\pi 4_{k4}(T)=(T[left] \oplus (Rot2(y)+y+1)) \parallel T[right]$

Key schedule

Let Dk be the data key.

Let Sk be the system key:

$Sk=s1 \parallel s2 \parallel \cdots \parallel s8$

where s1, s2, $\cdots$, s8 are 32-bit data blocks.

The work key Wk is obtained:

$a1=\pi 2_{s1} \cdot \pi 1(Dk)$

$w1=a1[left]$

$a2=\pi 3_{s2,s3}(a1)$

$w2=a2[right]$

$a3=\pi 4_{s4}(a2)$

$w3=a3[left]$

$a4=\pi 1(a3)$

$w4=a4[right]$

$a5=\pi 2_{s5}(a4)$

$w5=a5[left]$

$a6=\pi 3_{s6,s7}(a5)$

$w6=a6[right]$

$a7=\pi 4_{s8}(a6)$

$w7=a7[left]$

$a8=\pi 1(a7)$

$w8=a8[right]$

$Wk=w1 \parallel w2 \parallel \cdots \parallel w8$

Encryption

Let Wk be the work key:

$Wk=w1 \parallel w2 \parallel \cdots \parallel w8$

Let P be the plaintext. Let $N=8m+\alpha$ ($0 \leqq \alpha \leqq 7$) be the round number.

Then, the ciphertext C is obtained as follows:

Let f_{Wk} be the function:

$f_{Wk}=\pi 4_{w8} \cdot \pi 3_{w6,w7} \cdot \pi 2_{w5} \cdot \pi 1 \cdot \pi 4_{w4} \cdot \pi 3_{w2,w3} \cdot \pi 2_{w1} \cdot \pi 1$

Let F_{Wk} be the function:

$F_{Wk}=f_{Wk} \cdot f_{Wk} \cdot \cdots \cdot f_{Wk}$

where the calculation of f_{Wk} is repeated m times.

If $\alpha=0$, then

$C=F_{Wk}(P)$

If $\alpha=1$, then

$C=\pi 1 \cdot F_{Wk}(P)$

If $\alpha=2$, then

$C=\pi 2_{w1} \cdot \pi 1 \cdot F_{Wk}(P)$

If $\alpha=3$, then

$C=\pi 3_{w2,w3} \cdot \pi 2_{w1} \cdot \pi 1 \cdot F_{Wk}(P)$

If $\alpha=4$, then

$C=\pi 4_{w4} \cdot \pi 3_{w2,w3} \cdot \pi 2_{w1} \cdot \pi 1 \cdot F_{Wk}(P)$

If $\alpha=5$, then

$C=\pi 1 \cdot \pi 4_{w4} \cdot \pi 3_{w2,w3} \cdot \pi 2_{w1} \cdot \pi 1 \cdot F_{Wk}(P)$

If $\alpha=6$, then

$C=\pi 2_{w5} \cdot \pi 1 \cdot \pi 4_{w4} \cdot \pi 3_{w2,w3} \cdot \pi 2_{w1} \cdot \pi 1 \cdot F_{Wk}(P)$

If $\alpha=7$, then

$C=\pi 3_{w6,w7} \cdot \pi 2_{w5} \cdot \pi 1 \cdot \pi 4_{w4} \cdot \pi 3_{w2,w3} \cdot \pi 2_{w1} \cdot \pi 1 \cdot F_{Wk}(P)$

Decryption

The inverse function of f_{Wk} is obtained as:

$f_{Wk}^{-1}=\pi 1 \cdot \pi 2_{w1} \cdot \pi 3_{w2,w3} \cdot \pi 4_{w4} \cdot \pi 1 \cdot \pi 2_{w5} \cdot \pi 3_{w6,w7} \cdot \pi 4_{w8}$

Then, the inverse function of F_{Wk} is obtained as:

$F_{Wk}^{-1}=f_{Wk}^{-1} \cdot f_{Wk}^{-1} \cdot \cdots \cdot f_{Wk}^{-1}$

where the calculation of f_{Wk}^{-1} is repeated m times.

Then, the plaintext P is obtained as follows:

If $\alpha=0$, then

$P=F_{Wk}^{-1}(C)$

If $\alpha=1$, then

$P=F_{Wk}^{-1} \cdot \pi 1(C)$

If $\alpha=2$, then

$P=F_{Wk}^{-1} \cdot \pi 1 \cdot \pi 2_{w1}(C)$

If $\alpha=3$, then

$P=F_{Wk}^{-1} \cdot \pi 1 \cdot \pi 2_{w1} \cdot \pi 3_{w2,w3}(C)$

If $\alpha=4$, then

$P=F_{Wk}^{-1} \cdot \pi 1 \cdot \pi 2_{w1} \cdot \pi 3_{w2,w3} \cdot \pi 4_{w4}(C)$

If $\alpha=5$, then

$P=F_{Wk}^{-1} \cdot \pi 1 \cdot \pi 2_{w1} \cdot \pi 3_{w2,w3} \cdot \pi 4_{w4} \cdot \pi 1(C)$

If $\alpha=6$, then

$P=F_{Wk}^{-1} \cdot \pi 1 \cdot \pi 2_{w1} \cdot \pi 3_{w2,w3} \cdot \pi 4_{w4} \cdot \pi 1 \cdot \pi 2_{w5}(C)$

If $\alpha=7$, then

$P=F_{Wk}^{-1} \cdot \pi 1 \cdot \pi 2_{w1} \cdot \pi 3_{w2,w3} \cdot \pi 4_{w4} \cdot \pi 1 \cdot \pi 2_{w5} \cdot \pi 3_{w6,w7}(C)$