SXAL / MBAL

(a) ISO entry name

~~###~~ {iso standard 9979 sxal-mbal (12)}

(b) Proprietary entry name

Substitution Xor ALgorithm (SXAL)

Multi Block Algorithm (MBAL)

(c) Intended range of applications

confidentiality

authentication (as detailed in ISO 9798)

data integrity (as detailed in ISO 9797)

digital signature (as detailed in ISO 9796)

hash function

(d) Criptographic interface parameters

execution function code	2 byte
execution result code	2 byte
argorithm ciassify code	1 byte
encryption/decryption mode code	1 byte
data length	2 byte
key	8 byte
input data (SXAL/MBAL)	8 byte/8～1024 byte
output data (SXAL/MBAL)	8 byte/8～1024 byte

(e) Test words

SXAL	key (Hex)	31 32 33 34 35 36 37 38
	input data (Hex)	31 31 31 31 31 31 31 31
	output data (Hex)	0E 3A 3E DB 76 CF 46 1E
MBAL	reference to ohter sheet	

(f) The identity of the organization Sponsoring Authority

Information-technology Promotion Agency,japan (IPA)

Syuwa-shibakoen 3-chome Bldg.,6F

3-1-38 Shibakoen Minato-ku Tokyo 105,JAPAN

Tel +81-3-3437-2301 Fax +81-3-3437-9427

Registration Requested by
Laurel Intelligent Systems co.,ltd.
1-14-5 Azamino Aoba-ku Yokohama 225,JAPAN
Tel +81-45-901-4311 Fax +81-45-901-9969

(g) Dates of registration and modifications
~~NIL~~ 23 October 1995

(h) Whether the subject of a National Standard
N/A

(i) Patent license restrications
United States Patent No.5267313
Japan Trademark No.3037901
Japan Trademark No.3037902

(k) Description of algorithm
reference to other sheet
announced to "Institute of Electronics,Information and Communication Engineers,japan (ICE)" in Dec.1993

(e) Test words

MBAL key (Hex) 31 32 33 34 35 36 37 38

input data (Hex)	output data (Hex)
31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31	3A 5C B1 0C A6 55 5B 35 9A 92 EB EE A4 8C 8C 2C
31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31	64 15 9F 2C A5 C0 09 DF F3 81 8E 74 01 5F 6F 01
31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31	9D CB ED 4F 34 1E 6B 19 3B 37 FB 8D 8E 95 16 72
31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31	C4 AE F1 13 CD 4D E9 BA 06 9E 0B 20 6A 4E 09 5A
31 31 31 31 31 0D 0A 32 32 32 32 32 32 32 32 32	A5 21 54 2C 7E AB AC AC 66 E0 7F 26 9E 00 16 35
32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32	1F 6B 16 06 F9 8C 52 7B 1E 91 0A 3F DC 8C 6D 76
32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32	66 D7 79 BA 60 26 EC FB 46 6F 35 93 DF 59 38 C9
32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32	F6 08 BF F3 9C D0 FB 9A 3F 75 7B 5E BE 92 D2 A2
32 32 32 32 32 32 32 32 32 32 32 32 0D 0A 33 33	60 9E B3 F8 15 08 EB EB 57 93 38 B0 90 55 06 B4
33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33	D8 90 E6 B7 D5 C1 51 59 AF 60 14 9B 83 D8 38 C5
33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33	82 A6 DA 8C 94 72 53 D4 CF F9 69 B7 A9 5E 4B 0F
33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33	DD 72 91 D1 15 14 AD 7F E2 A2 6D 9F 32 B0 31 C0
33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33	AC D3 1B 33 BC CD 1B 0D 85 6A B4 F7 FF 53 13 A6
33 33 33 0D 0A 34 34 34 34 34 34 34 34 34 34 34	A9 A4 E5 86 5F DB AB 04 E9 6C 32 A6 56 48 46 E7
34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34	90 08 88 A8 E9 34 F3 FD B0 1F B1 2B 4B 47 5E 8B
34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34	2F B0 40 EA CA 5E 46 B7 02 EC 17 9E 33 C5 CD BA
34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34	90 2B 84 B7 7F BA BC 3B F3 53 D4 02 A2 B1 B8 28
34 34 34 34 34 34 34 34 34 34 0D 0A 35 35 35 35	6D 81 56 9A 0C 05 6C 5A DF 74 D9 BB 10 52 1E 1C
35 35 35 35 35 35 35 35 35 35 35 35 35 35 35 35	BF F0 41 8A 82 58 16 49 08 F5 FC C9 04 31 EC C2
35 35 35 35 35 35 35 35 35 35 35 35 35 35 35 35	E6 0C DD 48 29 D3 04 14 2E ED 27 5D BB 8D FD FE
35 35 35 35 35 35 35 35 35 35 35 35 35 35 35 35	55 7E CF EC C4 0D A1 C3 28 63 CE 28 12 8E 31 01
35 35 35 35 35 35 35 35 35 35 35 35 35 35 35 35	B0 C2 CC 97 54 C6 D3 BF 45 48 D1 C4 C0 24 4B C5
35 0D 0A 36 36 36 36 36 36 36 36 36 36 36 36 36	CD D6 26 D2 B0 DA C1 FA 65 6E 35 32 31 89 45 93
36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36	DE AF 14 81 92 88 59 73 9C 6F 94 7A DE 30 DA 46
36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36	9D 69 ED FC 6C CA BA C8 EA 97 A5 E2 58 11 6E 22
36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36	58 AD D3 6B 75 2D C8 97 E1 7C A3 5D 37 DB AA AB
36 36 36 36 36 36 36 0D 0A 37 37 37 37 37 37 37	99 6F 19 6F 9B DC DB F6 0D 0C C3 4B 90 51 92 C6
37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37	6A AB DA 4E 9D A4 FC 2C C1 8A F4 5D A3 C6 1D AA
37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37	36 0F C0 DE AF 9F 8F ED 5F B0 DE 8E 22 3F 94 A4
37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37	E2 20 E9 AF B5 2D E9 10 09 4A 19 C2 71 A8 EB 03
37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 0D	0D 5D 80 15 1F 55 B5 2E 38 E8 27 B4 9D 12 D2 DD
0A 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38	93 94 FA CB 11 40 F6 72 85 7E 2E 42 48 5B F1 2E
38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38	17 7D 11 2A CA 33 74 8A C2 F1 3C B4 17 F1 EE E8
38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38	24 C7 BE C6 00 A5 A4 74 64 68 E7 7F 9A 9D 06 8A
38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38	3A 3D C0 63 0B 20 26 33 14 B3 E9 B7 82 48 E4 F3
38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38	3F DC F9 57 44 9E ED 8D E7 65 F1 19 22 4B 94 6E
38 38 38 38 38 38 0D 0A 39 39 39 39 39 39 39 39	FD B3 3D 85 62 B1 89 2F B1 A6 FF F0 F6 CC B5 35
39 39 39 39 39 39 39 39 39 39 39 39 39 39 39 39	47 6D 89 03 E9 8A 49 42 6E D3 CE AF DA B1 B4 FC
39 39 39 39 39 39 39 39 39 39 39 39 39 39 39 39	D2 42 68 8F BB 6E 51 FD 8E 74 A0 08 E1 6E CB 75
39 39 39 39 39 39 39 39 39 39 39 39 39 39 39 39	DC EF D1 D6 5B BF C7 67 49 6E EE 56 2E 02 4B CB
39 39 39 39 39 39 39 39 39 39 39 39 0D 0A 30	15 9D 5B 9F DE A6 68 AF 96 D1 BB 7C 25 8B 8C 81
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	5A B6 00 B7 6A A1 7B 50 2E 5E D7 D2 CC 40 DF C1
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	86 35 47 66 51 1F 8A AF ED A8 B6 66 F1 57 55 B0
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	16 25 E7 09 6A FD A1 B2 D7 53 54 D3 D5 18 BC 9C
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	D4 E3 DD 76 64 EB 9B 15 6E 17 83 8E 38 78 5C 8B
30 30 30 30 0D 0A 61 61 61 61 61 61 61 61 61 61	CD CF 9C D8 AC 54 27 D0 21 00 4D 92 3C BB DA AF
61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61	63 9E D5 18 1B 40 06 C5 51 05 7D 0B 0A E6 96 EC
61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61	6A 85 FF FE DB CF 4D A3 86 25 1A 30 57 DA F6 39
61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61	97 22 9B BF FC AA FD 42 27 ED 87 95 D0 20 37 2E
61 61 61 61 61 61 61 61 61 61 61 0D 0A 62 62 62	4A 5B F7 AE 72 30 1F EF 5B 68 3D DF CA B7 F8 47
62 62 62 62 62 62 62 62 62 62 62 62 62 62 62 62	9C 18 65 64 AD 36 A8 DC 2E 65 79 CE D0 7E 39 2C
62 62 62 62 62 62 62 62 62 62 62 62 62 62 62 62	C3 A2 BC 9E A5 C0 8D BA DD 3E 59 48 C8 81 B1 C8
62 62 62 62 62 62 62 62 62 62 62 62 62 62 62 62	A3 94 F0 49 BF FB 8D 3F 26 4B 7F C7 D8 EA C6 60
62 62 62 62 62 62 62 62 62 62 62 62 62 62 62 62	F3 C4 BA 76 87 DC 1D E1 00 55 50 DE 9A 5E CB A9
62 62 0D 0A 63 63 63 63 63 63 63 63 63 63 63 63	DD 96 16 2C D2 5E 1E 99 82 4F E6 8D B0 E0 64 AC
63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63	FF 39 1D DE A6 3F D2 0C 5F D3 EB F4 D2 0C A2 62
63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63	63 87 BB 67 1F FF 01 05 B7 C3 B8 96 6A B3 EB 43
63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63	6B 9A 2D 03 82 A0 78 09 E0 31 3F BF AC 73 F8 53
63 63 63 63 63 63 63 63 0D 0A 64 64 64 64 64 64	9E D1 55 93 4B A6 78 FD 06 5C D5 09 D0 C6 1B 1F
64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64	6F B2 40 21 28 55 78 91 F1 7A 2E 24 E8 11 D5 C3
64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64	B5 AB 6A 08 8E C3 6D 3E 1A ED 5E 05 01 25 FA 80
64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64	F4 35 B0 0B 88 C1 F5 D0 34 E9 35 7A 74 F3 EC 79
64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64	34 41 19 97 26 5C 5B 3E 63 D6 75 48 F3 70 79 B9
0D 0A 66 66 66 66 66 66 66 66 66 66 66 66 66 66	B5 46 8A D8 32 A8 6C FB 31 51 C0 EA 67 05 82 3D
66 66 66 66 66 66 66 66 66 66 66 66 66 0D 0A 1A	

SXAL /MBAL algorithm

1. Preface

In the encryption technology, there is a category called as public algorithm with common encryption key methodology. In the United States, the standard technology is called as "DES". In Japan, NTT announced "FEAL" as an equivalent technology. Here, we have a technology called "SXAL ". These methodologies are called as "Block encryption algorithm" which use 8 bytes as one block of data.

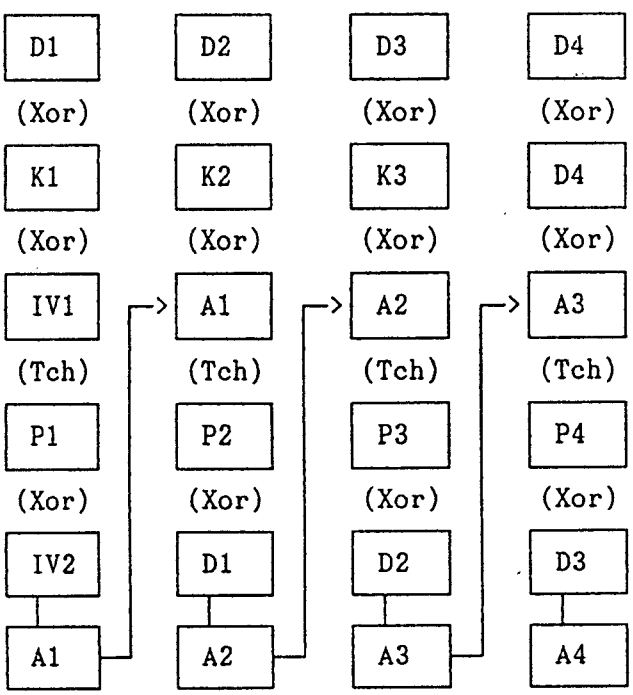
SXAL is slightly different from these two methods but basically, they are similar. It is also the block encryption process which handles 8 bytes as one block too. The advantage of this is that, by the use of basic "SXAL " algorithm, we can provide further flexible and therefore, it is advanced multi-block algorithm that does not limit the block size as 8 bytes.

The new algorithm is called "MBAL", which can provide faster process. This is beneficial for larger size of data to be encrypted faster. The "MBAL" will assist this method with accelerated encryption procedure by providing variable times of data processing steps.

Note: SXAL and MBAL are the registered trade mark by Laurel Intelligent Systems.

2. Basic algorithm

2-1. Basic algorithm



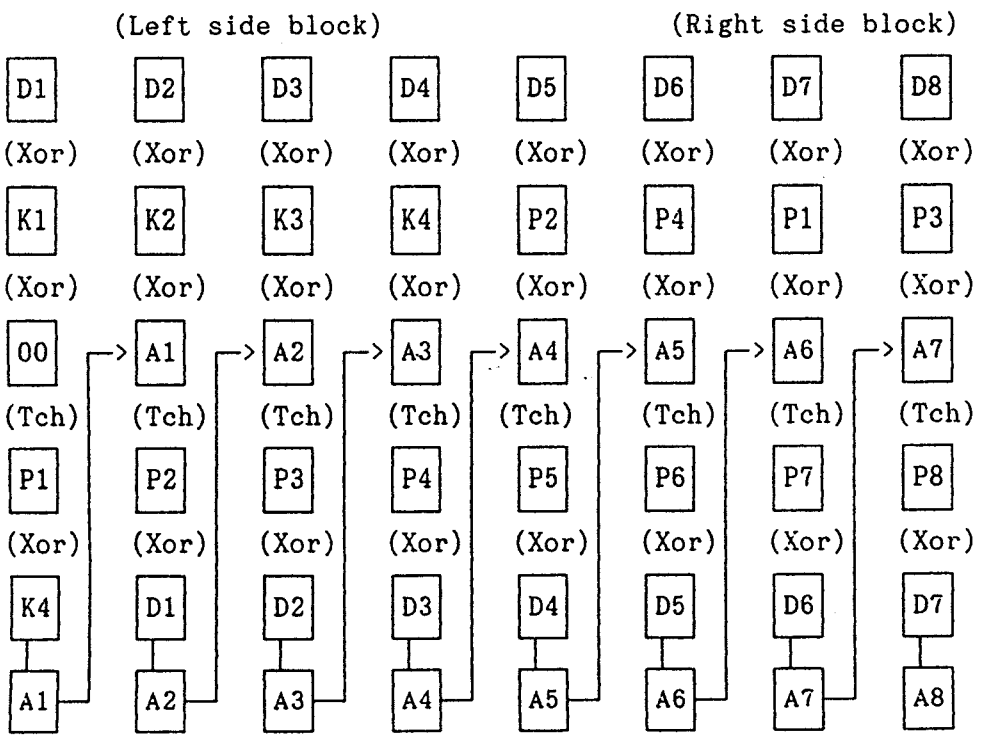
where (Xor)=exclusive OR operation and
(Tch)= character transposing operation by the use of conversion table.
On the above example, D1-D4 means input 4 bytes of data, K1-K4 means internal key 4 bytes and P1-P4 means variable key 4 bytes.

Therefore, A1 = D1(Xor)K1(Xor)IV1(Tch)(Xor)IV2 means A1 is the result of operation of at first, D1(Xor)K1(Xor)IV1 with the character transposing and then, applied (Xor) operation with IV2.

The algorithm is executed from left block to right. The execution chain is linked by passing the input data and its result from one process to the next. In the above example, IV1 will use "00h" and IV2 will use "K4" for the value.

2-2. One unit process step of basic algorithm.

In SXAL , one unit process step is consisted of two block process with basic algorithm.



In case of 8 bytes of block encryption, it will be divided into each 4 blocks. In the above example, left block of process will use internal key, K1 to K4 for encryption process. Right 4 blocks of encryption process will then use the resulted contents of P1 to P4. (The sequence will be, P2, P4, P1 and P3.)

IV1 of right side block will use A4 for its value and IV2 will use the content of K4 for its value. IV1 of left block will use "00h" for its value and IV2 will use the content of K4 for its value.

2-3. Two character translation table

In encryption process of "SXAL ", it will use two tables. One is used to encrypt the plain text file and the other is used to decrypt the encrypted text file back to plain text file. The latter is also called "Reverse table" and both are consisted of 256 bytes of characters.

These tables seemed random number table at a first glance but they should satisfy one condition mentioned below. There are several tables that satisfy these conditions and therefore, shown example is not unique one.

The condition means, "the resulted value of exclusive OR operation between the character of before translation and after the translation must be unique. There is none of other character that generates same exclusive OR value after the operation."

I.E. [X (Xor) K(X)] (Neq) [X' (Xor) K(X')]

where X' is the character after translation of X by translation table, (Xor) means exclusive OR operation and (Neq) means "Not equal" condition for both sides.

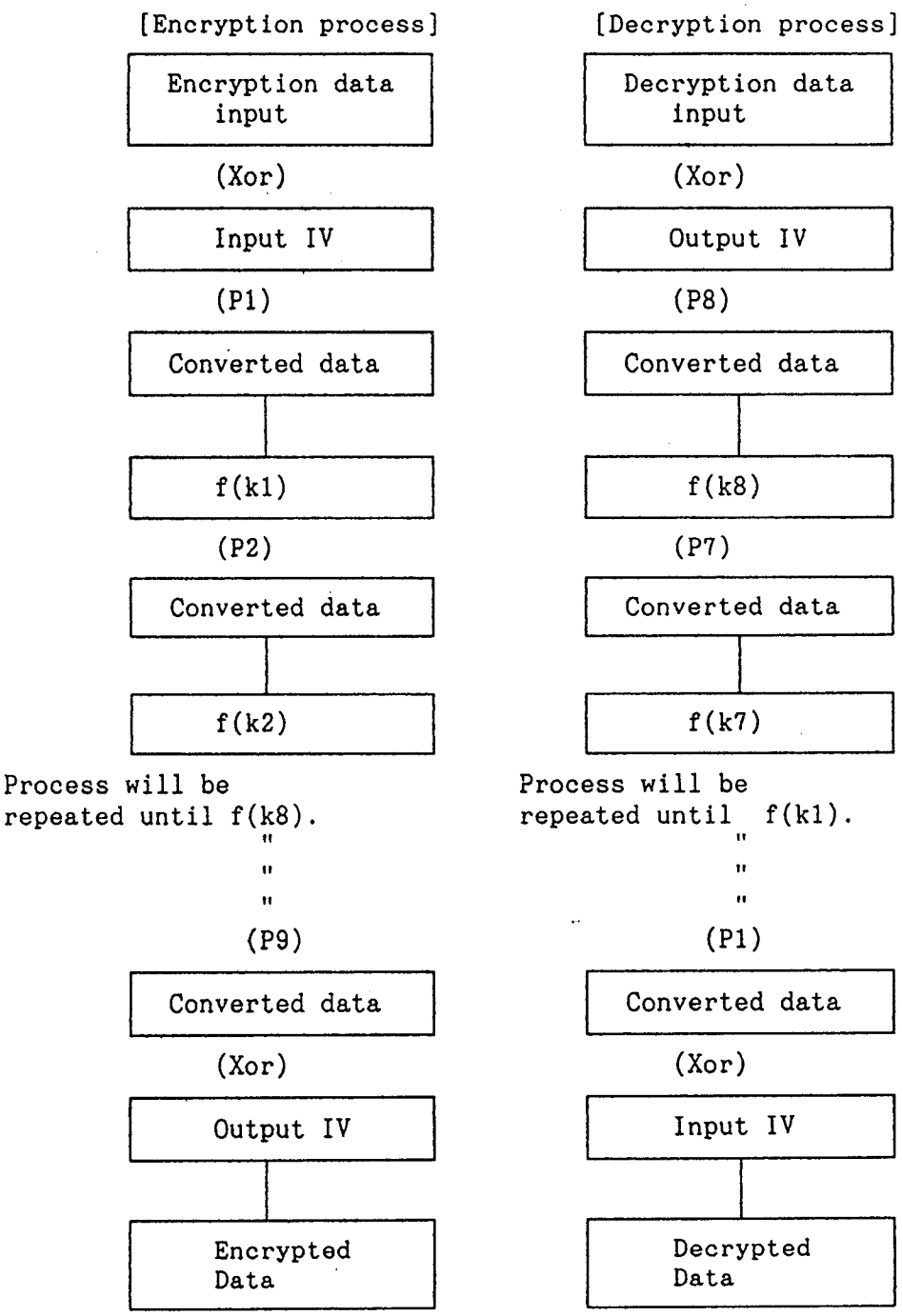
For example, "00h" will generates "1Eh" based on the conversion table. Therefore, the operation will be shown as:
00h (Xor) = 1Eh

So, the value, "1Eh" should be unique in the table.

The examples of normal tables used for encyption process and reverse table used for decrypting process will be shown in the attachement.

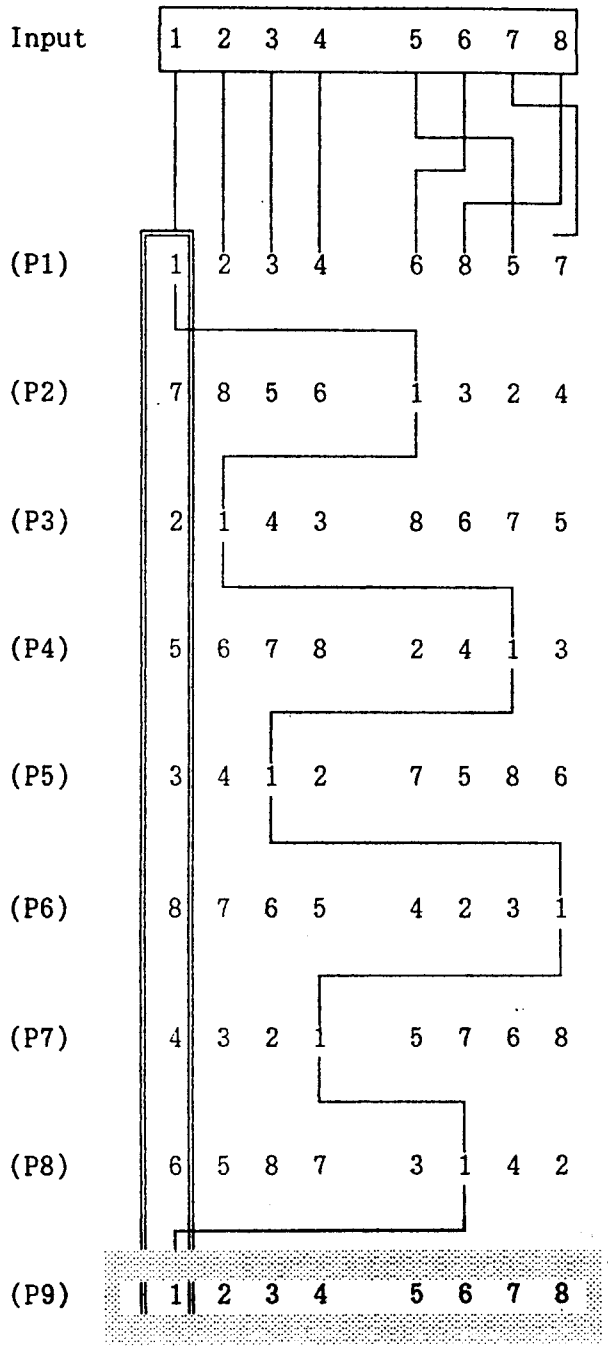
3. SXAL block encryption process

3-1. SXAL data scrambling process will be performed as shown below.



Where (Xor) means exclusive OR operation, (Pi) means byte transposition operation, f(ki) means basic algorithm and ki:i=1 to 8 means internal key.

3-2. Transposition operation at each input conversion stage.



3-3. Preprocess of key (Generating internal key)

Preprocess of key means the generation of internal key and IV (Initial variable) by scrambling data process. At the starting, key itself will be used as data and internal key and IV will use all "NUL" value for them. At the each stage, use extracted result from previous stage and extract the value for internal key (ki) and supply it to the following stage.

The chart shows how to extract the value by the operation of f(ki) to the right.

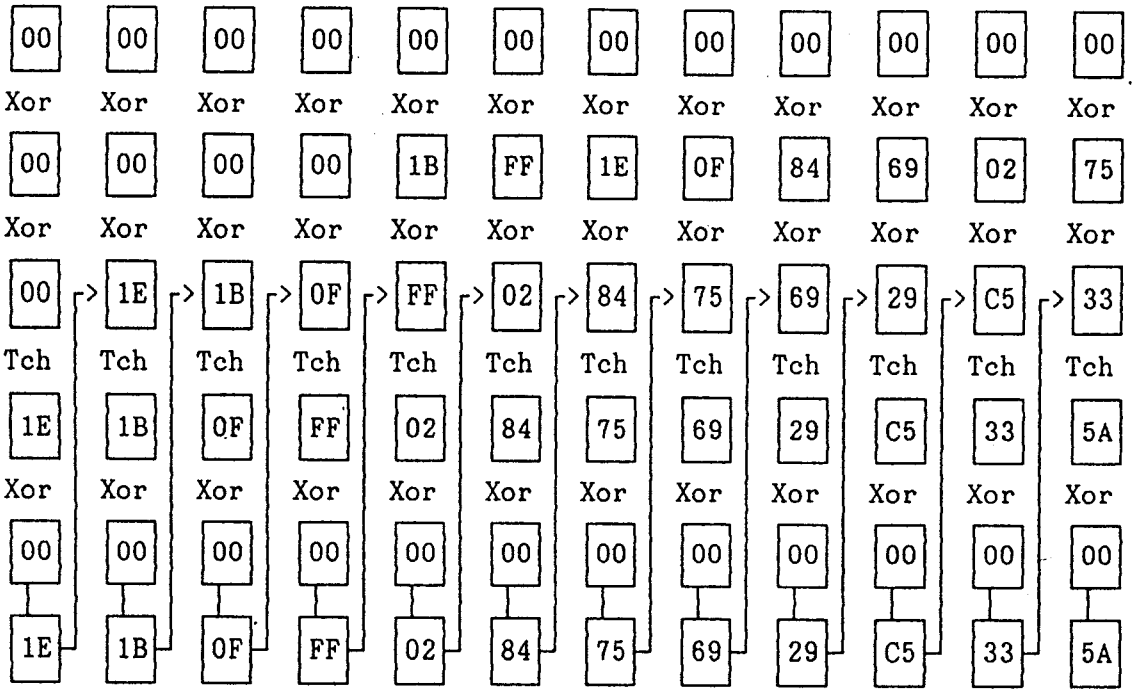
		k1	k3	k5		k7	in IV	out IV
k1 step	1	2	3	4	6	8	5	7
k2 step	7	8	5	6	1	3	2	4
k3 step	2	1	4	3	8	6	7	5
k4 step	5	6	7	8	2	4	1	3
k5 step	3	4	1	2	7	5	8	6
k6 step	8	7	6	5	4	2	3	1
k7 step	4	3	2	1	5	7	6	8
k8 step	6	5 k2	8 k4	7 k6	3	1 k8	4	2

At k1, from 1 to 4th stage, it will take second byte from the left and therefore, in the above chart, it will result "2 8 1 6".

4. MBAL as Multi-block algorithm

4-1. Extended use of basic algorithm in MBAL.

In the basic algorithm, it is chaining variable key to 1 block 4 bytes. In "SXAL ", the variable key is applied to 2 blocks and therefore, it enables to apply longer input data a group. For instance, the example shown below means the basic algorithm was applied one step of process for all "NUL" 12 bytes of data.



where Xor means exclusive or and Tch means character translation.

As explained in the example, variable key is generated based on the value supplied at initial input regardless the size of input data group. MBAL will require 8 stages of process and in "SXAL ", it will try to perform the same process within 3 stages.

4-2. Encryption process of MBAL

Following chart will explain the process with 16 bytes of input data.

(1) Step 1

<- 4 bytes ->

D1	D2	D3	D4

These are the input blocks. Onto 8 bytes of data in D1 and D2, this step will generate output IV used for "SXAL " and perform exclusive or operation. The result is shown below.

d1	d2	D3	D4

(2) Step 2

Apply basic algorithm onto d1,d2,D3 and D4. The sequence is d1,d2,D3 and D4. The key initially applied in this operation is k8 which will be used in "SXAL " process. The result is shown below.

A1	A2	A3	A4

(3) Step 3
Apply "SXAL " block encryption process onto A1 and A4 among A1,A2,A3 and A4. The result is shown below.

E1	A2	A3	E4

(4) Step 4
Apply basic algorithm onto E1,A2,A3 and E4. The sequence is E4,A3,A2 and E1. The initial key applied on this operation k7 which will be used in "SXAL ". The result is shown below.

B1	B2	B3	B4

(5) Step 5
Apply "SXAL " block encryption process onto B1 and B4 among B1,B2,B3 and B4. The result is shown below.

e1	B2	B3	e4

(6) Step 6
Apply basic algorithm onto e1,B2,B3 and e4. The sequence is e1,B2,B3 and e4. The initial key applied on this operation k6 which will be used in "SXAL ". The result is shown below.

X1	X2	X3	X4

(7) Step 7

Onto 8 bytes of data in X1 and X2, this step will generate input IV used for "SXAL " and perform exclusive or operation. The result is the encrypted output for D1,D2,D3 and D4. The result is shown below.

x1	x2	X3	X4

There are the differences between "SXAL " and "MBAL" operation for the use of internal key at each stage. And there are also the differences in the usage of input IV and output IV too.

For "MBAL", data length is not necessarily being the multiplication of number 4. Attention is suggested that in the operation, in the process of "SXAL ", it takes 4 bytes from each end of the block and perform block encryption process.

Attachment

Normal table used for data encryption process.

\ Upper 4 \ bits \-- Lower 4 \ bits \	b8	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
	b7	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
	b6	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
	b5	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
b4	b3	b2	b1	HX	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	1E	8C	4A	39	C5	FC	8A	41	4F	2A	55	C0	9E	0D	CA	BA
0	0	0	1	1	68	27	3C	F4	F7	B9	CF	EA	82	18	EF	6B	E8	A6	BC	00
0	0	1	0	2	D0	35	59	80	83	10	99	25	09	93	46	D3	FA	C3	73	56
0	0	1	1	3	7B	43	F2	B2	4E	AA	23	53	3B	5E	03	A5	51	B5	D8	13
0	1	0	0	4	C7	EE	28	5B	94	07	42	32	96	E2	37	08	65	5C	02	C9
0	1	0	1	5	0A	54	E5	2D	3F	71	34	88	E0	49	9C	3A	20	6E	47	62
0	1	1	0	6	81	FD	91	48	5A	63	FB	DE	58	F1	8E	B1	89	1A	11	AD
0	1	1	1	7	B3	B8	A3	E3	2C	C8	50	9B	F3	87	F8	7C	33	D7	AB	DB
1	0	0	0	8	52	6A	06	DF	01	92	6C	A7	21	66	19	26	D2	EB	86	7E
1	0	0	1	9	24	C1	70	9A	BB	5F	A1	0C	64	DC	2B	8D	A4	40	F0	4C
1	0	1	0	A	36	79	BF	CC	ED	D4	D5	69	CD	75	A0	9F	1C	8F	95	38
1	0	1	1	B	9D	0F	14	76	A8	E6	E7	1F	77	30	6D	E9	B7	F9	3E	F5
1	1	0	0	C	A9	A2	CE	17	72	4B	0E	F6	DA	04	D1	44	0B	98	E4	2F
1	1	0	1	D	EC	90	8B	61	D9	3D	78	C4	AC	AF	7A	FE	C6	22	29	84
1	1	1	0	E	45	1B	DD	AE	16	85	1D	B0	BE	BD	C2	57	4D	74	5D	E1
1	1	1	1	F	FF	D6	67	05	60	2E	B6	7D	15	CB	B4	12	7F	31	6F	97

Attachment

Reverse table used for data decripting process.

\ Upper 4 \ bits \-- Lower 4 bits \				b8	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
				b7	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
				b6	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
				b5	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
b4	b3	b2	b1	HX	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	F1	52	C5	9B	D9	67	4F	29	32	1D	AA	7E	B0	02	85	E9
0	0	0	1	1	48	E6	88	DF	70	C3	3D	55	06	26	69	B6	19	AC	FE	96
0	0	1	0	2	E4	BF	DD	74	64	08	F5	4C	81	58	1C	33	AE	C8	94	23
0	0	1	1	3	A3	F3	63	C7	13	73	56	E2	42	92	27	07	D2	B2	37	87
0	1	0	0	4	9C	2B	09	65	BC	15	89	DE	FD	44	C9	AF	7D	5A	EC	31
0	1	0	1	5	3F	8F	72	12	0E	A0	C4	9A	5E	EA	B3	D3	40	6A	25	FB
0	1	1	0	6	28	4E	B8	0A	A2	F2	98	3B	E8	84	D1	6F	CD	1F	5B	7C
0	1	1	1	7	54	3C	11	A4	E5	BE	2F	8B	97	FF	78	CB	04	D7	6B	41
1	0	0	0	8	B4	91	24	FA	36	86	01	6D	75	DC	4B	17	57	E3	C1	A7
1	0	0	1	9	82	A8	ED	30	95	22	7A	1A	C6	62	0C	51	F4	4D	BB	DB
1	0	1	0	A	05	D6	90	B5	20	46	18	AD	60	39	53	F0	E0	8C	71	C2
1	0	1	1	B	CC	1E	A9	83	5C	34	B1	03	2D	77	E7	49	9F	F7	D8	66
1	1	0	0	C	79	CA	47	21	F9	D4	68	B7	10	A5	8D	E1	3A	99	0D	50
1	1	0	1	D	D0	6E	35	5D	CE	EE	AB	7F	B9	0B	F6	9E	8A	2E	4A	16
1	1	1	0	E	6C	00	5F	EB	43	93	D5	F8	A6	C0	3E	8E	2C	76	14	BD
1	1	1	1	F	1B	7B	FC	45	80	59	EF	CF	DA	BA	9D	2A	61	38	A1	0F