Network Working Group
Request for Comments: 4009
Category: Informational

J. Park
S. Lee
J. Kim
J. Lee
KISA

February 2005

The SEED Encryption Algorithm

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document describes the SEED encryption algorithm, which has been adopted by most of the security systems in the Republic of Korea. Included are a description of the cipher and the key scheduling algorithm (Section 2), the S-boxes (Appendix A), and a set of test vectors (Appendix B).

1. Introduction

1.1. SEED Overview

SEED is a 128-bit symmetric key block cipher that has been developed by KISA (Korea Information Security Agency) and a group of experts since 1998. SEED is a national standard encryption algorithm in South Korea [TTASSEED] and is designed to use the S-boxes and permutations that balance with the current computing technology. It has the Feistel structure with 16-round and is strong against DC (Differential Cryptanalysis), LC (Linear Cryptanalysis), and related key attacks, balanced with security/efficiency trade-off.

The features of SEED are outlined as follows:

- The Feistel structure with 16-round
- 128-bit input/output data block size
- 128-bit key length
- A round function strong against known attacks
- Two 8x8 S-boxes
- Mixed operations of XOR and modular addition

SEED has been widely used in South Korea for confidential services such as electronic commerce; e.g., financial services provided in wired and wireless communication.

1.2. Notation

The following notation is used in the description of the SEED encryption algorithm:

&	bitwise AND
^	bitwise exclusive OR
+	addition in modular 2**32
-	subtraction in modular 2**32
||	concatenation
<< n	left circular rotation by n bits
>> n	right circular rotation by n bits
0x	hexadecimal representation

2. The Structure of SEED

The input/output block size of SEED is 128-bit, and the key length is also 128-bit. SEED has the 16-round Feistel structure. A 128-bit input is divided into two 64-bit blocks (L, R), and the right 64-bit block is an input to the round function F, with a 64-bit subkey Ki generated from the key schedule.

A pseudo code for the structure of SEED is as follows:

```
for (i = 1; i <= 16; i++)
{
  L = R;
  R = L ^ F(Ki, R);
}
```

2.1. The Round Function F

SEED uses two 8x8 S-boxes, permutations, rotations, and basic modular operations such as exclusive OR (XOR) and additions to provide strong security, high speed, and simplicity in its implementation.

A 64-bit input block of the round function F is divided into two 32-bit blocks (R0, R1) and wrapped with 4 phases:

- A mixing phase of two 32-bit subkey blocks (Ki0 , Ki1)
- 3 layers of function G (See Section 2.2), with additions for mixing two 32-bit blocks

The outputs (R0', R1') of function F are as follows:

```
R0' = G[ G[ G[(R0 ^ Ki0) ^ (R1 ^ Ki1)] + (R0 ^ Ki0)] + G[(R0 ^ Ki0)
       ^ (R1 ^ Ki1)]] + G[ G[(R0 ^ Ki0) ^ (R1 ^ Ki1)] + (R0 ^ Ki0)]

R1' = G[ G[ G[(R0 ^ Ki0) ^ (R1 ^ Ki1)] + (R0 ^ Ki0)] + G[(R0 ^ Ki0)
       ^ (R1 ^ Ki1)]] + G[ G[(R0 ^ Ki0) ^ (R1 ^ Ki1)]
```

2.2. The Function G

The function G has two layers: a layer of two 8x8 S-boxes and a layer of block permutation of sixteen 8-bit sub-blocks. The outputs Z (= Z0 || Z1 || Z2 || Z3) of the function G with four 8-bit inputs X (= X0 || X1 || X2 || X3) are as follows:

```
Z0 = {S1(X0) & m0} ^ {S2(X1) & m1} ^ {S1(X2) & m2} ^ {S2(X3) & m3}
Z1 = {S1(X0) & m1} ^ {S2(X1) & m2} ^ {S1(X2) & m3} ^ {S2(X3) & m0}
Z2 = {S1(X0) & m2} ^ {S2(X1) & m3} ^ {S1(X2) & m0} ^ {S2(X3) & m1}
Z3 = {S1(X0) & m3} ^ {S2(X1) & m0} ^ {S1(X2) & m1} ^ {S2(X3) & m2}
```

where m0 = 0xfc, m1 = 0xf3, m2 = 0xcf, and m3 = 0x3f.

To increase the efficiency of G function, four extended S-boxes 'SS-box' (See Appendix A.2) are defined as follows:

```
SS0(X)= {S1(X) & m3} || {S1(X) & m2} || {S1(X) & m1} || {S1(X) & m0}
SS1(X)= {S2(X) & m0} || {S2(X) & m3} || {S2(X) & m2} || {S2(X) & m1}
SS2(X)= {S1(X) & m1} || {S1(X) & m0} || {S1(X) & m3} || {S1(X) & m2}
SS3(X)= {S2(X) & m2} || {S2(X) & m1} || {S2(X) & m0} || {S2(X) & m3}
```

New G function, Z, can be defined as follows:

```
Z = SS0(X0) ^ SS1(X1) ^ SS2(X2) ^ SS3(X3)
```

This new G function is faster than the original G function but takes more memory to store four SS-boxes.

2.3. Key Schedule

The key schedule generates each round subkeys. It uses the function G, addition in modular 2**32, subtraction in modular 2**32, and (left/right) circular rotation. A 128-bit input key is divided into four 32-bit blocks (Key0, Key1, Key2, Key3). The two 32-bit subkeys of the ith round, Ki0 and Ki1, are generated as follows:

- Type 1 : Odd round
  Ki0 = G(Key0 + Key2 - KCi)
  Ki1 = G(Key1 - Key3 + KCi)
  Key0 || Key1 = (Key0 || Key1) >> 8

- Type 2 : Even round
  Ki0 = G(Key0 + Key2 - KCi)
  Ki1 = G(Key1 - Key3 + KCi)
  Key2 || Key3 = (Key2 || Key3) << 8

The following table shows constants used in KCi:

i	Value	i	Value
KC1	0x9e3779b9	KC2	0x3c6ef373
KC3	0x78dde6e6	KC4	0xf1bbcdcc
KC5	0xe3779b99	KC6	0xc6ef3733
KC7	0x8dde6e67	KC8	0x1bbcdccf
KC9	0x3779b99e	KC10	0x6ef3733c
KC11	0xdde6e678	KC12	0xbbcdccf1
KC13	0x779b99e3	KC14	0xef3733c6
KC15	0xde6e678d	KC16	0xbcdccf1b

A pseudo code for the key schedule is as follows:

```
for (i = 1; i <= 16; i++)
{
  Ki0 = G(Key0 + Key2 - KCi);
  Ki1 = G(Key1 - Key3 + KCi);

  if (i % 2 == 1)
    Key0 || Key1 = (Key0 || Key1) >> 8;
  else
    Key2 || Key3 = (Key2 || Key3) << 8;
}
```

2.4. Decryption Procedure

Decryption procedure is the reverse step of the encryption procedure. It can be implemented by using the encryption algorithm with reverse order of the round subkeys.

2.5. SEED Object Identifiers

For those who may be using SEED in algorithm negotiation within a protocol, or in any other context that may require the use of OIDs, the following three OIDs have been defined.

```
algorithm OBJECT IDENTIFIER ::=
  { iso(1) member-body(2) korea(410) kisa(200004) algorithm(1) }

id-seedCBC OBJECT IDENTIFIER ::= { algorithm seedCBC(4) }

seedCBCParameter ::= OCTET STRING  -- 128-bit Initialization Vector
```

The id-seedCBC OID is used when the CBC mode of operation based on the SEED block cipher is provided.

```
id-seedMAC OBJECT IDENTIFIER ::= { algorithm seedMAC(7) }

seedMACParameter ::= INTEGER  -- MAC length, in bits
```

The id-seedMAC OID is used when the message authentication code (MAC) algorithm based on the SEED block cipher is provided.

```
pbeWithSHA1AndSEED-CBC OBJECT IDENTIFIER ::=
  { algorithm seedCBCwithSHA1(15) }

PBEParameters ::= SEQUENCE {
  salt          OCTET STRING,
  iteration     INTEGER }  -- Total number of hash iterations
```

This OID is used when a password-based encryption in CBC mode based on SHA-1 and the SEED block cipher is provided. The details of the PBE computation are well described in Section 6.1 of [RFC2898].

3. Security Considerations

No security problem has been found on SEED. See [ISOSEED] and [CRYPTREC].

4. References

4.1. Normative References

[TTASSEED] Telecommunications Technology Association (TTA), "128-bit Symmetric Block Cipher (SEED)", TTAS.KO-12.0004, September, 1998 (In Korean) http://www.tta.or.kr/English/new/main/index.htm

[RFC2898] Kaliski, B., "PKCS #5: Password-Based Cryptography Specification Version 2.0", RFC 2898, September 2000.

4.2. Informative References

[ISOSEED] ISO/IEC, ISO/IEC JTC1/SC 27 N 256r1, "National Body contributions on NP 18033 Encryption algorithms in response to document SC 27 N 2563", October, 2000

[CRYPTREC] Information-technology Promotion Agency (IPA), Japan, CRYPTREC. "SEED Evaluation Report", February, 2002 http://www.kisa.or.kr/seed/seed_eng.html

Appendix A. S-Boxes

A.1. S-Boxes(two original S-boxes)

- S-Box S0

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

- S-Box S1

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

A.2. S-Boxes (four extended S-boxes)

- S-Box SS0

2989a1a8,05858184,16c6d2d4,13c3d3d0,14445054,1d0d111c,2c8ca0ac,25052124,
1d4d515c,03434340,18081018,1e0e121c,11415150,3cccf0fc,0acac2c8,23436360,
28082028,04444044,20002020,1d8d919c,20c0e0e0,22c2e2e0,08c8c0c8,17071314,
2585a1a4,0f8f838c,03030300,3b4b7378,3b8bb3b8,13031310,12c2d2d0,2ecee2ec,
30407070,0c8c808c,3f0f333c,2888a0a8,32023230,1dcdd1dc,36c6f2f4,34447074,
2ccce0ec,15859194,0b0b0308,17475354,1c4c505c,1b4b5358,3d8db1bc,01010100,
24042024,1c0c101c,33437370,18889098,10001010,0cccc0cc,32c2f2f0,19c9d1d8,
2c0c202c,27c7e3e4,32427270,03838380,1b8b9398,11c1d1d0,06868284,09c9c1c8,
20406060,10405050,2383a3a0,2bcbe3e8,0d0d010c,3686b2b4,1e8e929c,0f4f434c,
3787b3b4,1a4a5258,06c6c2c4,38487078,2686a2a4,12021210,2f8fa3ac,15c5d1d4,
21416160,03c3c3c0,3484b0b4,01414140,12425250,3d4d717c,0d8d818c,08080008,
1f0f131c,19899198,00000000,19091118,04040004,13435350,37c7f3f4,21c1e1e0,
3dcdf1fc,36467274,2f0f232c,27072324,3080b0b0,0b8b8388,0e0e020c,2b8ba3a8,
2282a2a0,2e4e626c,13839390,0d4d414c,29496168,3c4c707c,09090108,0a0a0208,
3f8fb3bc,2fcfe3ec,33c3f3f0,05c5c1c4,07878384,14041014,3ecef2fc,24446064,
1eced2dc,2e0e222c,0b4b4348,1a0a1218,06060204,21012120,2b4b6368,26466264,
02020200,35c5f1f4,12829290,0a8a8288,0c0c000c,3383b3b0,3e4e727c,10c0d0d0,
3a4a7278,07474344,16869294,25c5e1e4,26062224,00808080,2d8da1ac,1fcfd3dc,
2181a1a0,30003030,37073334,2e8ea2ac,36063234,15051114,22022220,38083038,
34c4f0f4,2787a3a4,05454144,0c4c404c,01818180,29c9e1e8,04848084,17879394,
35053134,0bcbc3c8,0ecec2cc,3c0c303c,31417170,11011110,07c7c3c4,09898188,
35457174,3bcbf3f8,1acad2d8,38c8f0f8,14849094,19495158,02828280,04c4c0c4,
3fcff3fc,09494148,39093138,27476364,00c0c0c0,0fcfc3cc,17c7d3d4,3888b0b8,
0f0f030c,0e8e828c,02424240,23032320,11819190,2c4c606c,1bcbd3d8,2484a0a4,
34043034,31c1f1f0,08484048,02c2c2c0,2f4f636c,3d0d313c,2d0d212c,00404040,
3e8eb2bc,3e0e323c,3c8cb0bc,01c1c1c0,2a8aa2a8,3a8ab2b8,0e4e424c,15455154,
3b0b3338,1cccd0dc,28486068,3f4f737c,1c8c909c,18c8d0d8,0a4a4248,16465254,
37477374,2080a0a0,2dcde1ec,06464244,3585b1b4,2b0b2328,25456164,3acaf2f8,
23c3e3e0,3989b1b8,3181b1b0,1f8f939c,1e4e525c,39c9f1f8,26c6e2e4,3282b2b0,
31013130,2acae2e8,2d4d616c,1f4f535c,24c4e0e4,30c0f0f0,0dcdc1cc,08888088,
16061214,3a0a3238,18485058,14c4d0d4,22426260,29092128,07070304,33033330,
28c8e0e8,1b0b1318,05050104,39497178,10809090,2a4a6268,2a0a2228,1a8a9298

- S-Box SS1

38380830,e828c8e0,2c2d0d21,a42686a2,cc0fcfc3,dc1eced2,b03383b3,b83888b0,
ac2f8fa3,60204060,54154551,c407c7c3,44044440,6c2f4f63,682b4b63,581b4b53,
c003c3c3,60224262,30330333,b43585b1,28290921,a02080a0,e022c2e2,a42787a3,
d013c3d3,90118191,10110111,04060602,1c1c0c10,bc3c8cb0,34360632,480b4b43,
ec2fcfe3,88088880,6c2c4c60,a82888a0,14170713,c404c4c0,14160612,f434c4f0,
c002c2c2,44054541,e021c1e1,d416c6d2,3c3f0f33,3c3d0d31,8c0e8e82,98188890,
28280820,4c0e4e42,f436c6f2,3c3e0e32,a42585a1,f839c9f1,0c0d0d01,dc1fcfd3,
d818c8d0,282b0b23,64264662,783a4a72,24270723,2c2f0f23,f031c1f1,70324272,
40024242,d414c4d0,40014141,c000c0c0,70334373,64274763,ac2c8ca0,880b8b83,
f437c7f3,ac2d8da1,80008080,1c1f0f13,c80acac2,2c2c0c20,a82a8aa2,34340430,
d012c2d2,080b0b03,ec2ecee2,e829c9e1,5c1d4d51,94148490,18180810,f838c8f0,
54174753,ac2e8ea2,08080800,c405c5c1,10130313,cc0dcdc1,84068682,b83989b1,
fc3fcff3,7c3d4d71,c001c1c1,30310131,f435c5f1,880a8a82,682a4a62,b03181b1,
d011c1d1,20200020,d417c7d3,00020202,20220222,04040400,68284860,70314171,
04070703,d81bcbd3,9c1d8d91,98198991,60214161,bc3e8eb2,e426c6e2,58194951,
dc1dcdd1,50114151,90108090,dc1cccd0,981a8a92,a02383a3,a82b8ba3,d010c0d0,
80018181,0c0f0f03,44074743,181a0a12,e023c3e3,ec2ccce0,8c0d8d81,bc3f8fb3,
94168692,783b4b73,5c1c4c50,a02282a2,a02181a1,60234363,20230323,4c0d4d41,
c808c8c0,9c1e8e92,9c1c8c90,383a0a32,0c0c0c00,2c2e0e22,b83a8ab2,6c2e4e62,
9c1f8f93,581a4a52,f032c2f2,90128292,f033c3f3,48094941,78384870,cc0cccc0,
14150511,f83bcbf3,70304070,74354571,7c3f4f73,34350531,10100010,00030303,
64244460,6c2d4d61,c406c6c2,74344470,d415c5d1,b43484b0,e82acae2,08090901,
74364672,18190911,fc3ecef2,40004040,10120212,e020c0e0,bc3d8db1,04050501,
f83acaf2,00010101,f030c0f0,282a0a22,5c1e4e52,a82989a1,54164652,40034343,
84058581,14140410,88098981,981b8b93,b03080b0,e425c5e1,48084840,78394971,
94178793,fc3cccf0,1c1e0e12,80028282,20210121,8c0c8c80,181b0b13,5c1f4f53,
74374773,54144450,b03282b2,1c1d0d11,24250521,4c0f4f43,00000000,44064642,
ec2dcde1,58184850,50124252,e82bcbe3,7c3e4e72,d81acad2,c809c9c1,fc3dcdf1,
30300030,94158591,64254561,3c3c0c30,b43686b2,e424c4e0,b83b8bb3,7c3c4c70,
0c0e0e02,50104050,38390931,24260622,30320232,84048480,68294961,90138393,
34370733,e427c7e3,24240420,a42484a0,c80bcbc3,50134353,080a0a02,84078783,
d819c9d1,4c0c4c40,80038383,8c0f8f83,cc0ecec2,383b0b33,480a4a42,b43787b3

- S-Box SS2

a1a82989,81840585,d2d416c6,d3d013c3,50541444,111c1d0d,a0ac2c8c,21242505,
515c1d4d,43400343,10181808,121c1e0e,51501141,f0fc3ccc,c2c80aca,63602343,
20282808,40440444,20202000,919c1d8d,e0e020c0,e2e022c2,c0c808c8,13141707,
a1a42585,838c0f8f,03000303,73783b4b,b3b83b8b,13101303,d2d012c2,e2ec2ece,
70703040,808c0c8c,333c3f0f,a0a82888,32303202,d1dc1dcd,f2f436c6,70743444,
e0ec2ccc,91941585,03080b0b,53541747,505c1c4c,53581b4b,b1bc3d8d,01000101,
20242404,101c1c0c,73703343,90981888,10101000,c0cc0ccc,f2f032c2,d1d819c9,
202c2c0c,e3e427c7,72703242,83800383,93981b8b,d1d011c1,82840686,c1c809c9,
60602040,50501040,a3a02383,e3e82bcb,010c0d0d,b2b43686,929c1e8e,434c0f4f,
b3b43787,52581a4a,c2c406c6,70783848,a2a42686,12101202,a3ac2f8f,d1d415c5,
61602141,c3c003c3,b0b43484,41400141,52501242,717c3d4d,818c0d8d,00080808,
131c1f0f,91981989,00000000,11181909,00040404,53501343,f3f437c7,e1e021c1,
f1fc3dcd,72743646,232c2f0f,23242707,b0b03080,83880b8b,020c0e0e,a3a82b8b,
a2a02282,626c2e4e,93901383,414c0d4d,61682949,707c3c4c,01080909,02080a0a,
b3bc3f8f,e3ec2fcf,f3f033c3,c1c405c5,83840787,10141404,f2fc3ece,60642444,
d2dc1ece,222c2e0e,43480b4b,12181a0a,02040606,21202101,63682b4b,62642646,
02000202,f1f435c5,92901282,82880a8a,000c0c0c,b3b03383,727c3e4e,d0d010c0,
72783a4a,43440747,92941686,e1e425c5,22242606,80800080,a1ac2d8d,d3dc1fcf,
a1a02181,30303000,33343707,a2ac2e8e,32343606,11141505,22202202,30383808,
f0f434c4,a3a42787,41440545,404c0c4c,81800181,e1e829c9,80840484,93941787,
31343505,c3c80bcb,c2cc0ece,303c3c0c,71703141,11101101,c3c407c7,81880989,
71743545,f3f83bcb,d2d81aca,f0f838c8,90941484,51581949,82800282,c0c404c4,
f3fc3fcf,41480949,31383909,63642747,c0c000c0,c3cc0fcf,d3d417c7,b0b83888,
030c0f0f,828c0e8e,42400242,23202303,91901181,606c2c4c,d3d81bcb,a0a42484,
30343404,f1f031c1,40480848,c2c002c2,636c2f4f,313c3d0d,212c2d0d,40400040,
b2bc3e8e,323c3e0e,b0bc3c8c,c1c001c1,a2a82a8a,b2b83a8a,424c0e4e,51541545,
33383b0b,d0dc1ccc,60682848,737c3f4f,909c1c8c,d0d818c8,42480a4a,52541646,
73743747,a0a02080,e1ec2dcd,42440646,b1b43585,23282b0b,61642545,f2f83aca,
e3e023c3,b1b83989,b1b03181,939c1f8f,525c1e4e,f1f839c9,e2e426c6,b2b03282,
31303101,e2e82aca,616c2d4d,535c1f4f,e0e424c4,f0f030c0,c1cc0dcd,80880888,
12141606,32383a0a,50581848,d0d414c4,62602242,21282909,03040707,33303303,
e0e828c8,13181b0b,01040505,71783949,90901080,62682a4a,22282a0a,92981a8a

- S-Box SS3

08303838,c8e0e828,0d212c2d,86a2a426,cfc3cc0f,ced2dc1e,83b3b033,88b0b838,
8fa3ac2f,40606020,45515415,c7c3c407,44404404,4f636c2f,4b63682b,4b53581b,
c3c3c003,42626022,03333033,85b1b435,09212829,80a0a020,c2e2e022,87a3a427,
c3d3d013,81919011,01111011,06020406,0c101c1c,8cb0bc3c,06323436,4b43480b,
cfe3ec2f,88808808,4c606c2c,88a0a828,07131417,c4c0c404,06121416,c4f0f434,
c2c2c002,45414405,c1e1e021,c6d2d416,0f333c3f,0d313c3d,8e828c0e,88909818,
08202828,4e424c0e,c6f2f436,0e323c3e,85a1a425,c9f1f839,0d010c0d,cfd3dc1f,
c8d0d818,0b23282b,46626426,4a72783a,07232427,0f232c2f,c1f1f031,42727032,
42424002,c4d0d414,41414001,c0c0c000,43737033,47636427,8ca0ac2c,8b83880b,
c7f3f437,8da1ac2d,80808000,0f131c1f,cac2c80a,0c202c2c,8aa2a82a,04303434,
c2d2d012,0b03080b,cee2ec2e,c9e1e829,4d515c1d,84909414,08101818,c8f0f838,
47535417,8ea2ac2e,08000808,c5c1c405,03131013,cdc1cc0d,86828406,89b1b839,
cff3fc3f,4d717c3d,c1c1c001,01313031,c5f1f435,8a82880a,4a62682a,81b1b031,
c1d1d011,00202020,c7d3d417,02020002,02222022,04000404,48606828,41717031,
07030407,cbd3d81b,8d919c1d,89919819,41616021,8eb2bc3e,c6e2e426,49515819,
cdd1dc1d,41515011,80909010,ccd0dc1c,8a92981a,83a3a023,8ba3a82b,c0d0d010,
81818001,0f030c0f,47434407,0a12181a,c3e3e023,cce0ec2c,8d818c0d,8fb3bc3f,
86929416,4b73783b,4c505c1c,82a2a022,81a1a021,43636023,03232023,4d414c0d,
c8c0c808,8e929c1e,8c909c1c,0a32383a,0c000c0c,0e222c2e,8ab2b83a,4e626c2e,
8f939c1f,4a52581a,c2f2f032,82929012,c3f3f033,49414809,48707838,ccc0cc0c,
05111415,cbf3f83b,40707030,45717435,4f737c3f,05313435,00101010,03030003,
44606424,4d616c2d,c6c2c406,44707434,c5d1d415,84b0b434,cae2e82a,09010809,
46727436,09111819,cef2fc3e,40404000,02121012,c0e0e020,8db1bc3d,05010405,
caf2f83a,01010001,c0f0f030,0a22282a,4e525c1e,89a1a829,46525416,43434003,
85818405,04101414,89818809,8b93981b,80b0b030,c5e1e425,48404808,49717839,
87939417,ccf0fc3c,0e121c1e,82828002,01212021,8c808c0c,0b13181b,4f535c1f,
47737437,44505414,82b2b032,0d111c1d,05212425,4f434c0f,00000000,46424406,
cde1ec2d,48505818,42525012,cbe3e82b,4e727c3e,cad2d81a,c9c1c809,cdf1fc3d,
00303030,85919415,45616425,0c303c3c,86b2b436,c4e0e424,8bb3b83b,4c707c3c,
0e020c0e,40505010,09313839,06222426,02323032,84808404,49616829,83939013,
07333437,c7e3e427,04202424,84a0a424,cbc3c80b,43535013,0a02080a,87838407,
c9d1d819,4c404c0c,83838003,8f838c0f,cec2cc0e,0b33383b,4a42480a,87b3b437

Appendix B. Test Vectors

This appendix provides test vectors for the SEED cipher described in this document.

B.1.

```
Key        : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Plaintext  : 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
Ciphertext : 5E BA C6 E0 05 4E 16 68 19 AF F1 CC 6D 34 6C DB
```

Intermediate Value

	K0	K1	L0	L1	R0	R1
Round 1	7C8F8C7E	C737A22C	00010203	04050607	08090A0B	0C0D0E0F
Round 2	FF276CDB	A7CA684A	08090A0B	0C0D0E0F	8081BC57	C4EA8A1F
Round 3	2F9D01A1	70049E41	8081BC57	C4EA8A1F	117A8B07	D7358C24
Round 4	AE59B3C4	4245E90C	117A8B07	D7358C24	D1738C94	7326CAB0
Round 5	A1D6400F	DBC1394E	D1738C94	7326CAB0	577ECE6D	1F8433EC
Round 6	85963508	0C5F1FCB	577ECE6D	1F8433EC	910F62AB	DDA096C1
Round 7	B684BDA7	61A4AEAE	910F62AB	DDA096C1	EA4D39B4	B17B1938
Round 8	D17E0741	FEE90AA1	EA4D39B4	B17B1938	B04E251F	97D7442C
Round 9	76CC05D5	E97A7394	B04E251F	97D7442C	B86D31BF	A5988C06
Round 10	50AC6F92	1B2666E5	B86D31BF	A5988C06	9008EABF	38DF7430
Round 11	65B7904A	8EC3A7B3	9008EABF	38DF7430	33E47DE0	54EFF76C
Round 12	2F7E2E22	A2B121B9	33E47DE0	54EFF76C	6BE9C434	BF3F378A
Round 13	4D0BFDE4	4E888D9B	6BE9C434	BF3F378A	B8DC3842	03A02D33
Round 14	631C8DDC	4378A6C4	B8DC3842	03A02D33	6679FCF7	9791DFCB
Round 15	216AF65F	7878C031	6679FCF7	9791DFCB	1A415792	A02B8C54
Round 16	71891150	98B255B0	1A415792	A02B8C54	19AFF1CC	6D346CDB

B.2.

```
   Key        : 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
   Plaintext  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   Ciphertext : C1 1F 22 F2 01 40 50 50 84 48 35 97 E4 37 0F 43
```

Intermediate Value

	K0	K1	L0	L1	R0	R1
Round 1 :	C119F584	5AE033A0	00000000	00000000	00000000	00000000
Round 2 :	62947390	A600AD14	00000000	00000000	9D8DB62C	911F0C19
Round 3 :	F6F6544E	596C4B49	9D8DB62C	911F0C19	21229A97	4AB4B7B8
Round 4 :	C1A3DE02	CE483C49	21229A97	4AB4B7B8	5A27B404	899D7315
Round 5 :	5E742E6D	7E25163D	5A27B404	899D7315	B8489E76	BA0EF3EA
Round 6 :	8299D2B4	790A46CE	B8489E76	BA0EF3EA	04A3DF29	31A27FB4
Round 7 :	EA67D836	55F354F2	04A3DF29	31A27FB4	EC9C17BF	81AA2AA0
Round 8 :	C47329FB	F50DB634	EC9C17BF	81AA2AA0	4FA74E8D	CDB21BB8
Round 9 :	2BD30235	51679CE6	4FA74E8D	CDB21BB8	D93492FE	4F71A4DA
Round 10 :	FA8D6B76	A9F37E02	D93492FE	4F71A4DA	B14053D9	A911379B
Round 11 :	8B99CC60	0F6092D4	B14053D9	A911379B	5A7024D6	3905668B
Round 12 :	BDAEFCFA	489C2242	5A7024D6	3905668B	605C8C3A	73DFBB75
Round 13 :	F6357C14	CFCCB126	605C8C3A	73DFBB75	40282F39	31CB8987
Round 14 :	A0AA6D85	F8C10774	40282F39	31CB8987	E9F834A8	3B9586D4
Round 15 :	47F4FEC5	353AE1BA	E9F834A8	3B9586D4	4B60324B	761C9958
Round 16 :	FECCEA48	A4EF9F9B	4B60324B	761C9958	84483597	E4370F43

B.3.

```
   Key        : 47 06 48 08 51 E6 1B E8 5D 74 BF B3 FD 95 61 85
   Plaintext  : 83 A2 F8 A2 88 64 1F B9 A4 E9 A5 CC 2F 13 1C 7D
   Ciphertext : EE 54 D1 3E BC AE 70 6D 22 6B C3 14 2C D4 0D 4A
```

Intermediate Value

	K0	K1	L0	L1	R0	R1
Round 1	56BE4A0F	E9F62877	83A2F8A2	88641FB9	A4E9A5CC	2F131C7D
Round 2	68BCB66C	078911DD	A4E9A5CC	2F131C7D	7CE5F012	47F8C1E6
Round 3	5B82740B	FD24D09B	7CE5F012	47F8C1E6	AAC99520	609F4CB7
Round 4	8D608015	A120E0BE	AAC99520	609F4CB7	3E126D1F	44FA99F0
Round 5	810A75AE	1BF223E5	3E126D1F	44FA99F0	11716365	9BA775AC
Round 6	F9C0D2D0	0F676C02	11716365	9BA775AC	32C9838F	BA5757CB
Round 7	8F9B5C84	8A7C8DDD	32C9838F	BA5757CB	77E00C64	CF9F6B32
Round 8	D4AB4896	18E93447	77E00C64	CF9F6B32	3F09B1F7	DE7D6D58
Round 9	CF090F51	5A4C8202	3F09B1F7	DE7D6D58	300E5CAA	D0BF2345
Round 10	4EC3196F	61B1A0DC	300E5CAA	D0BF2345	9574FDD7	4DF050D1
Round 11	244E07C1	D0D10B12	9574FDD7	4DF050D1	A15EDA6F	624265FD
Round 12	69917C6C	7FF94FB3	A15EDA6F	624265FD	9F39B682	D841C76F
Round 13	9A7EB482	723B5738	9F39B682	D841C76F	EEBBAD8B	C1F488EF
Round 14	B97522C5	39CC6349	EEBBAD8B	C1F488EF	45CF5D4E	BEEA4AA2
Round 15	FFC2AFD5	1412E731	45CF5D4E	BEEA4AA2	43B7FE1B	BCF87781
Round 16	A9AF7241	A3E67359	43B7FE1B	BCF87781	226BC314	2CD40D4A

B.4.

```
   Key        : 28 DB C3 BC 49 FF D8 7D CF A5 09 B1 1D 42 2B E7
   Plaintext  : B4 1E 6B E2 EB A8 4A 14 8E 2E ED 84 59 3C 5E C7
   Ciphertext : 9B 9B 7B FC D1 81 3C B9 5D 0B 36 18 F4 0F 51 22
```

Intermediate Value

	K0	K1	L0	L1	R0	R1
Round 1	B2B11B63	2EE9E2D1	B41E6BE2	EBA84A14	8E2EED84	593C5EC7
Round 2	11967260	71A62F24	8E2EED84	593C5EC7	1B31F2F7	3DDE00BA
Round 3	2E017A5A	35DAD7A7	1B31F2F7	3DDE00BA	35CC49C0	2AFB59EA
Round 4	1B2AB5FF	A3ADA69F	35CC49C0	2AFB59EA	D7AB53AA	AE82F1C7
Round 5	519C9903	DA90AAEE	D7AB53AA	AE82F1C7	24139958	B840E56F
Round 6	29FD95AD	B94C3F13	24139958	B840E56F	24AB5291	544C9DBA
Round 7	6F629D19	8ACE692F	24AB5291	544C9DBA	E8152994	75D0B424
Round 8	30A26E73	2F22338E	E8152994	75D0B424	A2CD1153	F32BB23A
Round 9	9721073A	98EE8DAE	A2CD1153	F32BB23A	C386008B	E3257731
Round 10	C597A8A9	27DCDC97	C386008B	E3257731	98396BFD	814F8972
Round 11	F5163A00	5FFD0003	98396BFD	814F8972	E74D2D0D	11D889D1
Round 12	5CBE65DA	A73403E4	E74D2D0D	11D889D1	29D8C7B3	D1B71C0C
Round 13	7D5CF070	1D3B8092	29D8C7B3	D1B71C0C	C4E692C2	D2F57F18
Round 14	388C702B	1BAA4945	C4E692C2	D2F57F18	2FAFB300	5F0C4BFF
Round 15	87D1AB5A	FA13FB5C	2FAFB300	5F0C4BFF	60E5F17C	5626BB68
Round 16	C97D7EED	90724A6E	60E5F17C	5626BB68	5D0B3618	F40F5122

Authors' Addresses

Jongwook Park
Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul, 138-803
REPUBLIC OF KOREA

Phone: +82-2-405-5432
FAX : +82-2-405-5499
EMail: khopri@kisa.or.kr

Sungjae Lee
Korea Information Security Agency

Phone: +82-2-405-5243
FAX : +82-2-405-5499
EMail: sjlee@kisa.or.kr

Jeeyeon Kim
Korea Information Security Agency

Phone: +82-2-405-5238
FAX : +82-2-405-5499
EMail: jykim@kisa.or.kr

Jaeil Lee
Korea Information Security Agency

Phone: +82-2-405-5300
FAX : +82-2-405-5499
EMail: jilee@kisa.or.kr

Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the IETF's procedures with respect to rights in IETF Documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.