Internet-Draft
Obsoletes: 4009(if approved)
Expires: November 2005

H.J. Lee
S.J. Lee
J.H. Yoon
D.H. Cheon
J.I. Lee
KISA

May 2005

The SEED Encryption Algorithm
<draft-lee-rfc4009bis-01.txt>

Status of this Memo

Copyright Notice

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 encryption and the key scheduling algorithm (Section 2), the S-boxes (Appendix A), and a set of test vectors (Appendix B).

1. Introduction

1.1. Changes from RFC 4009

This specification obsoletes RFC 4009, because the RFC 4009 had ambiguous function and SS-boxes definitions cryptographically. Thus, some definitions have been changed and for better understanding, the SEED pseudo codes have been modified. This update is to provide clarity and facilitate the development of interoperable implementations. The SEED algorithm itself has not been changed.

This specification updates the RFC 4009 in the following areas:

- Pseudo code changes. The Pseudo code in section2 in RFC4009 is insufficient for the explanation of the structure of SEED. Thus detailed pseudo code is introduced.

- Some corrections of errata which are the definition of R1', Z, X and SS-boxes.

1.2. SEED Overview

SEED is a 128-bit symmetric key block cipher that has been developed by KISA (Korea Information Security Agency) since 1998. SEED is a national standard encryption algorithm in the Republic of 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 the Republic of Korea for confidential services such as electronic commerce; e.g., financial services provided in wired and wireless communication.

1.3. 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:

```
Input : (L, R)

for i = 1 to 15
          L = R, R = L ^ F(Ki, R)

L = L ^ F(K16, R), R=R

Output : (L, 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)]]
```


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 (= Z3 || Z2 || Z1 || Z0) of the function G with four 8-bit inputs X (= X3 || X2 || X1 || X0) are as follows:

```
Z0 = {S0(X0) & m0} ^ {S1(X1) & m1} ^ {S0(X2) & m2} ^ {S1(X3) & m3}
Z1 = {S0(X0) & m1} ^ {S1(X1) & m2} ^ {S0(X2) & m3} ^ {S1(X3) & m0}
Z2 = {S0(X0) & m2} ^ {S1(X1) & m3} ^ {S0(X2) & m0} ^ {S1(X3) & m1}
Z3 = {S0(X0) & m3} ^ {S1(X1) & m0} ^ {S0(X2) & m1} ^ {S1(X3) & m2}
```

where m0 = 0xFC, m1 = 0xF3, m2 = 0xCF, and m3 = 0x3F.

To increase the efficiency of G function, four extended S-boxes

```
SS0(X0)= {S0(X0)& m3} || {S0(X0)& m2} || {S0(X0)& m1} || {S0(X0)& m0}
SS1(X1)= {S1(X1)& m0} || {S1(X1)& m3} || {S1(X1)& m2} || {S1(X1)& m1}
SS2(X2)= {S0(X2)& m1} || {S0(X2)& m0} || {S0(X2)& m3} || {S0(X2)& m2}
SS3(X3)= {S1(X3)& m2} || {S1(X3)& m1} || {S1(X3)& m0} || {S1(X3)& 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:

```
Input : (Key0, Key1, Key2, Key3)

for i = 1 to 16
  Ki0 = G(Key0 + Key2 - KCi)
  Ki1 = G(Key1 - Key3 + KCi)
  if i is odd
         Key0 || Key1 = (Key0 || Key1) >> 8
  esle
         Key2 || Key3 = (Key2 || Key3) << 8
```

```
        Output : (Keyi0, Keyi1), i=1 to 16
```

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 (SIZE(16))
  -- 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. Reference

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/data/Document_pdf/SEED_Evaluation_Report_by_CRYPTREC.pdf

5. Acknowledgments

Alfred Hoenes(ah@tr-sys.de) has contributed significantly to work on the definition of R1', Z, X and SS-boxes. Thanks for his contribution for this document.

6. Authors' Addresses

Hyangjin Lee
Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul, 138-803
REPUBLIC OF KOREA
Phone: +82-2-405-5446
FAX : +82-2-405-5319
EMail: jiinii@kisa.or.kr

Sungjae Lee
Korea Information Security Agency
Phone: +82-2-405-5243
FAX : +82-2-405-5499
EMail: sjlee@kisa.or.kr

Jaeho Yoon
Korea Information Security Agency
Phone: +82-2-405-5434
FAX : +82-2-405-5219
EMail: jhyoon@kisa.or.kr

Donghyeon Cheon
Korea Information Security Agency
Phone: +82-2-405-5251
FAX : +82-2-405-5319
EMail: dhcheon@kisa.or.kr

Jaeil Lee
Korea Information Security Agency
Phone: +82-2-405-5300
FAX : +82-2-405-5219
EMail: jilee@kisa.or.kr

Appendix A. S-Boxes

In this part, all data are hexadecimal numbers(not prefixed by "0x").

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.
All data are hexadecimal numbers(not prefixed by "0x").

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

	Ki0	Ki1	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

	Ki0	Ki1	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

	Ki0	Ki1	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

	Ki0	Ki1	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
```


Intellectual Property Statement

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 procedures with respect to rights in RFC 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.

Disclaimer of Validity

Copyright Statement

Acknowledgment

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