```
Test vectors for RSA PKCS#1 v1.5 Encryption
===========================================

This file contains test vectors for the PKCS#1 v1.5
encryption scheme. 15 RSA keys of different sizes have
been generated. For each key, 20 random messages of length
between 1 and 64 octets have been PKCS#1 v1.5 encrypted.
As specified in PKCS#1, the block type for this operation is 2.
The seed value of each example provides the pseudo random bytes
to be used for padding. This makes the result predictable.
Note that each example can be used to test encryption and
decryption.

Key lengths:

Key  1: 1024 bits
Key  2: 1024 bits
Key  3: 1024 bits
Key  4: 1024 bits
Key  5: 1024 bits
Key  6: 1024 bits
Key  7: 1025 bits
Key  8: 1026 bits
Key  9: 1027 bits
Key 10: 1028 bits
Key 11: 1029 bits
Key 12: 1030 bits
Key 13: 1031 bits
Key 14: 1536 bits
Key 15: 2048 bits

These test vectors have been derived from the OAEP test vectors.
===========================================================================
# Thirteen RSA keys with bit sizes between 1024 and 1031, one 1536-bit key,
# and one 2048-bit key are generated.

# For each key, 20 random messages are PKCS#1 v1.5 encrypted with random seeds.

# Example 1: A 1024-bit RSA key pair
# ------------------------------------------------------


# Public key
# ----------

# Modulus:
a8 b3 b2 84 af 8e b5 0b 38 70 34 a8 60 f1 46 c4
91 9f 31 87 63 cd 6c 55 98 c8 ae 48 11 a1 e0 ab
c4 c7 e0 b0 82 d6 93 a5 e7 fc ed 67 5c f4 66 85
12 77 2c 0c bc 64 a7 42 c6 c6 30 f5 33 c8 cc 72
f6 2a e8 33 c4 0b f2 58 42 e9 84 bb 78 bd bf 97
c0 10 7d 55 bd b6 62 f5 c4 e0 fa b9 84 5c b5 14
8e f7 39 2d d3 aa ff 93 ae 1e 6b 66 7b b3 d4 24
76 16 d4 f5 ba 10 d4 cf d2 26 de 88 d3 9f 16 fb

# Exponent:
01 00 01

# Private key
# -----------

# Modulus:
a8 b3 b2 84 af 8e b5 0b 38 70 34 a8 60 f1 46 c4
91 9f 31 87 63 cd 6c 55 98 c8 ae 48 11 a1 e0 ab
c4 c7 e0 b0 82 d6 93 a5 e7 fc ed 67 5c f4 66 85
12 77 2c 0c bc 64 a7 42 c6 c6 30 f5 33 c8 cc 72
f6 2a e8 33 c4 0b f2 58 42 e9 84 bb 78 bd bf 97
c0 10 7d 55 bd b6 62 f5 c4 e0 fa b9 84 5c b5 14
```



```
8e f7 39 2d d3 aa ff 93 ae 1e 6b 66 7b b3 d4 24
76 16 d4 f5 ba 10 d4 cf d2 26 de 88 d3 9f 16 fb

# Public exponent:
01 00 01

# Exponent:
53 33 9c fd b7 9f c8 46 6a 65 5c 73 16 ac a8 5c
55 fd 8f 6d d8 98 fd af 11 95 17 ef 4f 52 e8 fd
8e 25 8d f9 3f ee 18 0f a0 e4 ab 29 69 3c d8 3b
15 2a 55 3d 4a c4 d1 81 2b 8b 9f a5 af 0e 7f 55
fe 73 04 df 41 57 09 26 f3 31 1f 15 c4 d6 5a 73
2c 48 31 16 ee 3d 3d 2d 0a f3 54 9a d9 bf 7c bf
b7 8a d8 84 f8 4d 5b eb 04 72 4d c7 36 9b 31 de
f3 7d 0c f5 39 e9 cf cd d3 de 65 37 29 ea d5 d1

# Prime 1:
d3 27 37 e7 26 7f fe 13 41 b2 d5 c0 d1 50 a8 1b
58 6f b3 13 2b ed 2f 8d 52 62 86 4a 9c b9 f3 0a
f3 8b e4 48 59 8d 41 3a 17 2e fb 80 2c 21 ac f1
c1 1c 52 0c 2f 26 a4 71 dc ad 21 2e ac 7c a3 9d

# Prime 2:
cc 88 53 d1 d5 4d a6 30 fa c0 04 f4 71 f2 81 c7
b8 98 2d 82 24 a4 90 ed be b3 3d 3e 3d 5c c9 3c
47 65 70 3d 1d d7 91 64 2f 1f 11 6a 0d d8 52 be
24 19 b2 af 72 bf e9 a0 30 e8 60 b0 28 8b 5d 77

# Prime exponent 1:
0e 12 bf 17 18 e9 ce f5 59 9b a1 c3 88 2f e8 04
6a 90 87 4e ef ce 8f 2c cc 20 e4 f2 74 1f b0 a3
3a 38 48 ae c9 c9 30 5f be cb d2 d7 68 19 96 7d
46 71 ac c6 43 1e 40 37 96 8d b3 78 78 e6 95 c1

# Prime exponent 2:
95 29 7b 0f 95 a2 fa 67 d0 07 07 d6 09 df d4 fc
05 c8 9d af c2 ef 6d 6e a5 5b ec 77 1e a3 33 73
4d 92 51 e7 90 82 ec da 86 6e fe f1 3c 45 9e 1a
63 13 86 b7 e3 54 c8 99 f5 f1 12 ca 85 d7 15 83

# Coefficient:
4f 45 6c 50 24 93 bd c0 ed 2a b7 56 a3 a6 ed 4d
67 35 2a 69 7d 42 16 e9 32 12 b1 27 a6 3d 54 11
ce 6f a9 8d 5d be fd 73 26 3e 37 28 14 27 43 81
81 66 ed 7d d6 36 87 dd 2a 8c a1 d2 f4 fb d8 e1

# PKCS#1 v1.5 encryption of 20 random messages with random seeds
# ---------------------------------------------------------------------------

# ----------------------------------

# Message:
66 28 19 4e 12 07 3d b0 3b a9 4c da 9e f9 53 23
97 d5 0d ba 79 b9 87 00 4a fe fe 34

# Seed:
01 73 41 ae 38 75 d5 f8 71 01 f8 cc 4f a9 b9 bc
15 6b b0 46 28 fc cd b2 f4 f1 1e 90 5b d3 a1 55
d3 76 f5 93 bd 73 04 21 08 74 eb a0 8a 5e 22 bc
cc b4 c9 d3 88 2a 93 a5 4d b0 22 f5 03 d1 63 38
b6 b7 ce 16 dc 7f 4b bf 9a 96 b5 97 72 d6 60 6e
97 47 c7 64 9b f9 e0 83 db 98 18 84 a9 54 ab 3c
6f

# Encryption:
50 b4 c1 41 36 bd 19 8c 2f 3c 3e d2 43 fc e0 36
e1 68 d5 65 17 98 4a 26 3c d6 64 92 b8 08 04 f1
69 d2 10 f2 b9 bd fb 48 b1 2f 9e a0 50 09 c7 7d
```

```
a2 57 cc 60 0c ce fe 3a 62 83 78 9d 8e a0 e6 07
ac 58 e2 69 0e c4 eb c1 01 46 e8 cb aa 5e d4 d5
cc e6 fe 7b 0f f9 ef c1 ea bb 56 4d bf 49 82 85
f4 49 ee 61 dd 7b 42 ee 5b 58 92 cb 90 60 1f 30
cd a0 7b f2 64 89 31 0b cd 23 b5 28 ce ab 3c 31

# PKCS#1 v1.5 Encryption Example 1.2
# ----------------------------------

# Message:
75 0c 40 47 f5 47 e8 e4 14 11 85 65 23 29 8a c9
ba e2 45 ef af 13 97 fb e5 6f 9d d5

# Seed:
ac 47 28 a8 42 8c 1e 52 24 71 a8 df 73 5a 8e 92
92 af 0d 55 bc b7 3a 12 ac 32 c2 64 f3 88 1c 7c
8a 71 0f 70 fe b1 04 85 c8 37 0f 78 1f ff d0 21
81 6f 05 87 39 76 6d a0 a9 c9 db 0e ae 7e 9a 25
b6 c4 33 18 d0 ca ac 23 65 22 ca 31 0f 17 fc 52
ad 42 29 c8 3a 24 e9 e5 45 eb 35 e9 82 6d 55 9f
57

# Encryption:
68 42 e5 e2 cc 00 41 d6 b0 c8 1a 56 2c 39 a6 17
37 9a 51 5c ab 74 ab cb 26 19 c7 74 0a 54 1d 95
55 dd 91 65 97 5b f8 a3 eb d0 d0 45 66 61 df b1
a6 86 1b a2 33 22 69 93 0e 0d b5 14 fc a0 73 3e
eb 9c 40 57 13 eb 1f 9d 76 80 33 ed 29 3e 1e 08
1a 12 5f 32 dd b9 ea 52 ed be 27 5c 4a f6 0f 8a
7b f8 32 bd 22 75 61 c2 08 dc 00 31 a8 4b 50 12
c9 dd 9f 74 45 9d cb 07 0b db e1 3c fa 8c 2d 50

# PKCS#1 v1.5 Encryption Example 1.3
# ----------------------------------

# Message:
d9 4a e0 83 2e 64 45 ce 42 33 1c b0 6d 53 1a 82
b1 db 4b aa d3 0f 74 6d c9 16 df 24 d4 e3 c2 45
1f ff 59 a6 42 3e b0 e1 d0 2d 4f e6 46 cf 69 9d
fd 81 8c 6e 97 b0 51

# Seed:
dd 2d 60 a5 e0 08 eb e1 d0 be 6f 60 db c4 3f 29
62 ef 50 bf de 54 2b bb e9 8f ed d1 fe ac 05 7e
77 1c f1 5f c6 32 c8 db 27 2e 28 d2 9b 57 93 ea
6a b8 06 21 8c 53 82 39 b9 3a 93 5e 65 d2 44 16
ec 6c 6e 99 ae 04

# Encryption:
70 9c 7d 2d 45 98 c9 60 65 b6 58 8d a2 f8 9f a8
7f 06 2d 72 41 ef 65 95 89 8f 63 7a da 57 ea e9
01 73 f0 fb 4b f6 a9 1e bd 96 50 69 07 c8 53 da
cf 20 84 94 be 94 d3 13 a0 41 85 d4 74 a9 07 41
2e ff c3 e0 24 d0 7e 4d 09 aa 24 5f bc b1 30 21
9b fa 5d e0 2d 4f 7e 2e c9 e6 2e 8a d3 2d ee 5f
f4 d8 e4 cf ec bc 50 33 a1 c2 c6 1c 52 33 ae 16
19 2a 48 1d 00 75 bf c7 ce 02 82 12 cd 27 be be

# PKCS#1 v1.5 Encryption Example 1.4
# ----------------------------------

# Message:
52 e6 50 d9 8e 7f 2a 04 8b 4f 86 85 21 53 b9 7e
01 dd 31 6f 34 6a 19 f6 7a 85

# Seed:
26 29 a7 aa c0 c3 90 5e 83 1e b6 02 38 8c 54 5a
f5 54 b9 6b 2a e5 15 32 e9 cc db 89 72 ef 30 b6
```



```
4a 2f 98 c6 95 29 7a 01 c5 81 2a 2c 40 15 82 f3
7b 14 4a 3e 90 e5 9d 81 b6 90 39 c6 4b 84 4b 02
8c 10 5c 8e 68 36 15 af b6 58 b6 c4 d9 f3 82 38
a7 63 01 bb 14 44 91 13 b6 9d e1 26 04 5e 26 f1
3e e6 d7

# Encryption:
54 dd b7 84 26 8e ad b3 95 5b d9 f9 49 88 42 59
5a d2 9f f8 a6 67 fe b4 1f 6f 53 0c b6 0b c9 26
ac 6c 71 c7 72 f8 03 d0 22 b4 1c a5 72 04 22 3b
27 ca 79 ec 5b 72 65 2c a9 af bf 40 dc 2f 6a 0e
13 bc d6 0d 37 f7 95 04 b0 ff cc 01 cf 53 42 d6
d3 4a c6 f1 f2 f9 f2 f4 87 46 25 b9 fd bb 7d da
2e c8 7d f0 cf 87 25 97 98 df 86 a0 6b d5 ae f7
35 4b 8c b1 cb 13 75 75 f4 cf bc 46 28 1b b3 31

# PKCS#1 v1.5 Encryption Example 1.5
# ----------------------------------

# Message:
8d a8 9f d9 e5 f9 74 a2 9f ef fb 46 2b 49 18 0f
6c f9 e8 02

# Seed:
c3 ca 84 60 0f 35 c8 65 5f c7 c6 4c 75 c5 87 38
53 d3 aa 8a 94 26 a5 1b 63 d7 e7 5d cf 6c ae 97
a4 25 3f ba 87 1d 6f 96 89 97 19 9b f0 1b 6a 4d
34 28 ce 4c 96 d1 c4 87 b2 83 0c b9 e3 5d 64 05
56 23 69 9a b4 97 9a 02 58 4b 92 e6 ba 39 e7 57
28 40 79 ab f1 33 a7 da 54 e5 42 52 17 a2 10 f6
7c 18 26 9b 51 1f 61 f8 c5

# Encryption:
a8 55 48 01 3b d0 e2 0e e0 eb d3 6f b7 48 97 7f
98 58 46 d7 61 0e ed 24 c3 6c d8 30 33 dd 2a a4
58 0b d1 53 35 20 9d cf 78 2e e2 6c 48 c3 06 44
b0 b5 cc 86 c8 cd 16 5a e2 1e ad f5 78 04 18 67
76 07 03 18 75 e2 21 ec df 3b 10 57 31 6f 3f 12
a4 7d 5d a4 0c 41 53 9b 63 64 30 da 2e 54 21 90
11 9e 42 9c 53 c2 22 6f 95 9b 19 cc f4 8a 3d 24
02 17 c4 de 70 d7 07 2a 7e 0d 95 b6 16 d1 15 a8

# PKCS#1 v1.5 Encryption Example 1.6
# ----------------------------------

# Message:
26 52 10 50 84 42 71

# Seed:
3c 6a 04 71 da f0 0b 7c 2e fc 9e e8 80 41 65 4f
87 62 90 07 c1 24 32 22 11 a5 f4 ea 3c 58 23 85
7b c8 fc 7e 21 c9 45 48 b0 ee bd cf f7 91 60 e1
12 46 1e 40 50 91 10 cf dc 4f 0f 13 c7 fb 92 1a
ba c8 df aa c2 1a cb 0f 7b 8a 13 a4 b5 cc a5 23
d5 c7 dd f7 05 23 eb 57 0c 59 b6 c7 ae 97 67 e4
ec 9a 63 d1 13 6d 10 23 1b 40 1e 20 e7 41 02 84
83 48 01 7a 16 16

# Encryption:
5e 51 43 63 28 7d e9 b3 80 04 8c c4 43 5d 53 29
4a d5 94 1c 55 1a 97 e1 3c 16 dc 13 98 de 61 0d
c7 33 7b c6 bd e5 78 e9 e9 f5 6a f1 44 54 f2 e8
31 be ef 32 31 a8 50 68 e8 fe f7 2c 89 e1 df 1c
99 43 0a 60 f6 d9 42 89 cf ba 87 b2 b4 32 a4 0b
88 db 61 da e0 88 f9 ed 4e 28 4a 21 63 af 65 bf
2b 43 55 9a 5d a2 ae c5 bb 8f 43 f9 2c 1b 04 a5
14 6a 65 b6 e0 19 b4 cd d2 94 0c 35 d9 64 5b 2d
```

```
# PKCS#1 v1.5 Encryption Example 1.7
# ------------------------------------

# Message:
8a 84 7d d9 e2

# Seed:
a1 3d ff 8a 48 e8 04 94 ae 66 e6 ba 9f 17 9a 01
0d 9e 6d 40 31 87 96 7f 99 fd d9 0e f9 0e 0a 94
07 3f f0 e4 d0 e6 66 4f f3 73 b5 09 95 3e 04 ef
77 83 be 0f b4 6c 8a 9f c0 ed 8c 1f 33 cb 4d 0d
2f 1d 0d 5c db a1 4d ca 50 8c a1 d7 3d 20 80 18
63 9b c8 e1 65 86 23 de 1e 5b a3 f0 5e d0 91 4d
2f 96 90 2f 25 20 33 2d 84 92 d3 73 4a cd eb bd
f4 3e 50 a4 3e 7a a8 72

# Encryption:
82 7a 67 e8 15 78 1c 4d 4e 2b 2e 16 9d 80 ca e9
36 68 72 a7 92 af bf 3c 0c d5 1c e2 8c 70 e8 6d
41 eb b9 75 2f 3f 92 db a5 1a db b6 85 1b 1f 78
45 61 a8 f1 97 20 8f de 02 97 0b 38 f2 a9 74 22
ec 7f 4f c8 a1 06 75 a9 db de 10 9e ed 0c e0 65
27 70 3e e0 5b 65 7d 34 08 f7 fd db 1e ec cf fa
e1 6b 1d a1 07 30 7a 2c f2 56 fa 60 e8 15 21 72
de 9f 95 27 fe 92 0a 90 1d 93 c4 f4 d5 7e 54 6e

# PKCS#1 v1.5 Encryption Example 1.8
# ------------------------------------
```