Data##
#

    Keyed-Hash Message Authentication Code (HMAC)
        using SHA3-384

      Hashlen = 48

##

Sample #1

Block length = 104

Key length = 48

Tag length = 48

Input Data:
    "Sample message for keylen<blocklen"

Text is
    53616d70 6c65206d 65737361 67652066
    6f72206b 65796c65 6e3c626c 6f636b6c
    656e

Key is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    20212223 24252627 28292a2b 2c2d2e2f

K0 is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    20212223 24252627 28292a2b 2c2d2e2f
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000

K0 xor ipad is
    36373435 32333031 3e3f3c3d 3a3b3839
    26272425 22232021 2e2f2c2d 2a2b2829
    16171415 12131011 1e1f1c1d 1a1b1819
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636

```
    36363636 36363636 36363636 36363636
    36363636 36363636

Hash((Key^ipad)||text) is
    78800019 42f2b2c1 8e6794ec d4426868
    d004d03c e26d4ba4 a34ce9ee 088e0c0e
    32eb5ac2 3e4007cb 7253392b 3b4a5f33

K0 xor opad is
    5c5d5e5f 58595a5b 54555657 50515253
    4c4d4e4f 48494a4b 44454647 40414243
    7c7d7e7f 78797a7b 74757677 70717273
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    d588a3c5 1f3f2d90 6e8298c1 199aa8ff
    62962181 27f6b38a 90b6afe2 c5617725
    bc99987f 79b22a55 7b6520db 710b7f42

________________________________________________________________
Mac is
    d588a3c5 1f3f2d90 6e8298c1 199aa8ff
    62962181 27f6b38a 90b6afe2 c5617725
    bc99987f 79b22a55 7b6520db 710b7f42

================================================================

Sample #2

Block length = 104

Key length = 104

Tag length = 48

Input Data:
    "Sample message for keylen=blocklen"

Text is
    53616d70 6c65206d 65737361 67652066
    6f72206b 65796c65 6e3d626c 6f636b6c
    656e
```

```
Key is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    20212223 24252627 28292a2b 2c2d2e2f
    30313233 34353637 38393a3b 3c3d3e3f
    40414243 44454647 48494a4b 4c4d4e4f
    50515253 54555657 58595a5b 5c5d5e5f
    60616263 64656667
--------------------------------------------------------------
K0 is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    20212223 24252627 28292a2b 2c2d2e2f
    30313233 34353637 38393a3b 3c3d3e3f
    40414243 44454647 48494a4b 4c4d4e4f
    50515253 54555657 58595a5b 5c5d5e5f
    60616263 64656667

K0 xor ipad is
    36373435 32333031 3e3f3c3d 3a3b3839
    26272425 22232021 2e2f2c2d 2a2b2829
    16171415 12131011 1e1f1c1d 1a1b1819
    06070405 02030001 0e0f0c0d 0a0b0809
    76777475 72737071 7e7f7c7d 7a7b7879
    66676465 62636061 6e6f6c6d 6a6b6869
    56575455 52535051

Hash((Key^ipad)||text) is
    dd66b670 2b55fb9f 6614e310 12f1604a
    134a30d8 c1c97576 f1fae2a6 e5cd8a98
    8ad9c022 72063324 f97dc7b6 5dd02516

K0 xor opad is
    5c5d5e5f 58595a5b 54555657 50515253
    4c4d4e4f 48494a4b 44454647 40414243
    7c7d7e7f 78797a7b 74757677 70717273
    6c6d6e6f 68696a6b 64656667 60616263
    1c1d1e1f 18191a1b 14151617 10111213
    0c0d0e0f 08090a0b 04050607 00010203
    3c3d3e3f 38393a3b


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    a27d24b5 92e8c8cb f6d4ce6f c5bf62d8
    fc98bf2d 486640d9 eb8099e2 4047837f
    5f3bffbe 92dcce90 b4ed5b1e 7e44fa90
```

```
------------------------------------------------------------
Mac is
    a27d24b5 92e8c8cb f6d4ce6f c5bf62d8
    fc98bf2d 486640d9 eb8099e2 4047837f
    5f3bffbe 92dcce90 b4ed5b1e 7e44fa90

============================================================

Sample #3

Block length = 104

Key length = 152

Tag length = 48

Input Data:
    "Sample message for keylen>blocklen"

Text is
    53616d70 6c65206d 65737361 67652066
    6f72206b 65796c65 6e3e626c 6f636b6c
    656e

Key is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    20212223 24252627 28292a2b 2c2d2e2f
    30313233 34353637 38393a3b 3c3d3e3f
    40414243 44454647 48494a4b 4c4d4e4f
    50515253 54555657 58595a5b 5c5d5e5f
    60616263 64656667 68696a6b 6c6d6e6f
    70717273 74757677 78797a7b 7c7d7e7f
    80818283 84858687 88898a8b 8c8d8e8f
    90919293 94959697
------------------------------------------------------------
K0 is
    f8e53817 bff912a4 2876fd20 e35fd064
    a05f39ce 42deabef b435dcfa 2466b4ad
    b3c23765 f13bd31e 3dbb0005 d695055b
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000

K0 xor ipad is
    ced30e21 89cf2492 1e40cb16 d569e652
```

```
    96690ff8 74e89dd9 8203eacc 1250829b
    85f40153 c70de528 0b8d3633 e0a3336d
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636

Hash((Key^ipad)||text) is
    538c9ce0 66085c69 d2c296be ad5c5868
    e8a5e4fc cc20edf0 f21ca907 7959df73
    cc033bb6 5e8a6670 6bad8b79 7d89f906

K0 xor opad is
    a4b9644b e3a54ef8 742aa17c bf038c38
    fc036592 1e82f7b3 e86980a6 783ae8f1
    ef9e6b39 ad678f42 61e75c59 8ac95907
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    e5ae4c73 9f455279 368ebf36 d4f5354c
    95aa184c 899d3870 e460ebc2 88ef1f94
    70053f73 f7c6da2a 71bcaec3 8ce7d6ac

----------------------------------------------------------------
Mac is
    e5ae4c73 9f455279 368ebf36 d4f5354c
    95aa184c 899d3870 e460ebc2 88ef1f94
    70053f73 f7c6da2a 71bcaec3 8ce7d6ac

================================================================

Sample #4

Block length = 104

Key length = 48

Tag length = 24

Input Data:
    "Sample message for keylen<blocklen, with truncated tag"

Text is
```

```
    53616d70 6c65206d 65737361 67652066
    6f72206b 65796c65 6e3c626c 6f636b6c
    656e2c20 77697468 20747275 6e636174
    65642074 6167

Key is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    20212223 24252627 28292a2b 2c2d2e2f

________________________________________________________________
K0 is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    20212223 24252627 28292a2b 2c2d2e2f
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000

K0 xor ipad is
    36373435 32333031 3e3f3c3d 3a3b3839
    26272425 22232021 2e2f2c2d 2a2b2829
    16171415 12131011 1e1f1c1d 1a1b1819
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636

Hash((Key^ipad)||text) is
    5b38bc9b 912245a6 ce80e505 27187755
    5a7117c5 d9f4ff0a 8c2d282e 18ad6cc8
    8357ded8 1f1fe13e 7dc17a1c c88bc49f

K0 xor opad is
    5c5d5e5f 58595a5b 54555657 50515253
    4c4d4e4f 48494a4b 44454647 40414243
    7c7d7e7f 78797a7b 74757677 70717273
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    25f4bf53 606e91af 79d24a4b b1fd6aec
    d44414a3 0c8ebb0a e09764c7 1aceefe8
```

dfa72309 e48152c9 8294be65 8a33836e

Mac is
25f4bf53 606e91af 79d24a4b b1fd6aec
d44414a3 0c8ebb0a