Data##
#

    Keyed-Hash Message Authentication Code (HMAC)
        using SHA3-256

      Hashlen = 32

##

Sample #1

Block length = 136

Key length = 32

Tag length = 32

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

K0 is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    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
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636

```
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636

Hash((Key^ipad)||text) is
    b3c64b43 7d825ea2 2b35250c 50a167bd
    2cd41774 9aceb677 f7ab5c9f d2c518c0

K0 xor opad is
    5c5d5e5f 58595a5b 54555657 50515253
    4c4d4e4f 48494a4b 44454647 40414243
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    4fe8e202 c4f058e8 dddc23d8 c34e4673
    43e23555 e24fc2f0 25d598f5 58f67205

----------------------------------------------------------------
Mac is
    4fe8e202 c4f058e8 dddc23d8 c34e4673
    43e23555 e24fc2f0 25d598f5 58f67205

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

Sample #2

Block length = 136

Key length = 136

Tag length = 32

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 68696a6b 6c6d6e6f
    70717273 74757677 78797a7b 7c7d7e7f
    80818283 84858687
----------------------------------------------------------------
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 68696a6b 6c6d6e6f
    70717273 74757677 78797a7b 7c7d7e7f
    80818283 84858687

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 5e5f5c5d 5a5b5859
    46474445 42434041 4e4f4c4d 4a4b4849
    b6b7b4b5 b2b3b0b1

Hash((Key^ipad)||text) is
    c65e39b4 d2d01cf5 f8a0aab6 aa34e303
    c76e30c9 0dcb7b81 3f5917d3 319355e8

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 34353637 30313233
```

```
    2c2d2e2f 28292a2b 24252627 20212223
    dcdddedf d8d9dadb


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    68b94e2e 538a9be4 103bebb5 aa016d47
    961d4d1a a9060613 13b557f8 af2c3faa

----------------------------------------------------------------
Mac is
    68b94e2e 538a9be4 103bebb5 aa016d47
    961d4d1a a9060613 13b557f8 af2c3faa

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

Sample #3

Block length = 136

Key length = 168

Tag length = 32

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 98999a9b 9c9d9e9f
    a0a1a2a3 a4a5a6a7
----------------------------------------------------------------
K0 is
    369a33ba dfa618d5 8d16aadd eaff98d6
    6b30a70c 2deee42f c809b972 1dc1c524
```

```
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000

K0 xor ipad is
    00ac058c e9902ee3 bb209ceb dcc9aee0
    5d06913a 1bd8d219 fe3f8f44 2bf7f312
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636

Hash((Key^ipad)||text) is
    f962fde0 17872be1 a74e6e61 e3fee1ea
    06fff6f7 94d53c32 defd87c6 e413f508

K0 xor opad is
    6ac66fe6 83fa4489 d14af681 b6a3c48a
    376cfb50 71b2b873 9455e52e 419d9978
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    9bcf2c23 8e235c3c e88404e8 13bd2f3a
    97185ac6 f238c63d 6229a00b 07974258

________________________________________________________________
Mac is
    9bcf2c23 8e235c3c e88404e8 13bd2f3a
    97185ac6 f238c63d 6229a00b 07974258

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

Sample #4
```

```
Block length = 136

Key length = 32

Tag length = 16

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

------------------------------------------------------------
K0 is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000
    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
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636 36363636 36363636
    36363636 36363636

Hash((Key^ipad)||text) is
    2de533db 67c30604 818ff798 a3c6de8f
    868633da f55c1614 477c9ad1 12ef76db
```

```
K0 xor opad is
    5c5d5e5f 58595a5b 54555657 50515253
    4c4d4e4f 48494a4b 44454647 40414243
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
    5c5c5c5c 5c5c5c5c

Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    c8dc7148 d8c1423a a549105d afdf9cad
    2941471b 5c622070 88e56ccf 2dd80545

----------------------------------------------------------------
Mac is
    c8dc7148 d8c1423a a549105d afdf9cad
```