```
Data#############################################################
#

   Keyed-Hash Message Authentication Code (HMAC)
       using SHA3-512

     Hashlen = 64

##############################################################

Sample #1

Block length = 72

Key length = 64

Tag length = 64

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
   30313233 34353637 38393a3b 3c3d3e3f

--------------------------------------------------------------
K0 is
   00010203 04050607 08090a0b 0c0d0e0f
   10111213 14151617 18191a1b 1c1d1e1f
   20212223 24252627 28292a2b 2c2d2e2f
   30313233 34353637 38393a3b 3c3d3e3f
   00000000 00000000

K0 xor ipad is
   36373435 32333031 3e3f3c3d 3a3b3839
   26272425 22232021 2e2f2c2d 2a2b2829
   16171415 12131011 1e1f1c1d 1a1b1819
   06070405 02030001 0e0f0c0d 0a0b0809
   36363636 36363636
```

```
Hash((Key^ipad)||text) is
    7865df66 2f8577ba 01c208ff 369629c7
    f134ad57 4a0d1af3 bf31b444 3cc286a9
    4afb9d6f d1c4141b d61599e5 95bec0a6
    7f495e3e 6aa11f4d 89b16dab bf8e743b

K0 xor opad is
    5c5d5e5f 58595a5b 54555657 50515253
    4c4d4e4f 48494a4b 44454647 40414243
    7c7d7e7f 78797a7b 74757677 70717273
    6c6d6e6f 68696a6b 64656667 60616263
    5c5c5c5c 5c5c5c5c


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    4efd629d 6c71bf86 162658f2 9943b1c3
    08ce27cd fa6db0d9 c3ce8176 3f9cbce5
    f7ebe986 8031db1a 8f8eb7b6 b95e5c5e
    3f657a89 96c86a2f 6527e307 f0213196

--------------------------------------------------------------
Mac is
    4efd629d 6c71bf86 162658f2 9943b1c3
    08ce27cd fa6db0d9 c3ce8176 3f9cbce5
    f7ebe986 8031db1a 8f8eb7b6 b95e5c5e
    3f657a89 96c86a2f 6527e307 f0213196

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

Sample #2

Block length = 72

Key length = 72

Tag length = 64

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
--------------------------------------------------------------
K0 is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    20212223 24252627 28292a2b 2c2d2e2f
    30313233 34353637 38393a3b 3c3d3e3f
    40414243 44454647

K0 xor ipad is
    36373435 32333031 3e3f3c3d 3a3b3839
    26272425 22232021 2e2f2c2d 2a2b2829
    16171415 12131011 1e1f1c1d 1a1b1819
    06070405 02030001 0e0f0c0d 0a0b0809
    76777475 72737071

Hash((Key^ipad)||text) is
    30fb38f0 3679ce41 3e6f08e2 18b43102
    2b7ab1af 28984b95 2491bb57 8e671dd4
    deed7be8 4eb547f1 b5a23161 59a16250
    421b81e0 0a603daa 003fa541 f3d40b3c

K0 xor opad is
    5c5d5e5f 58595a5b 54555657 50515253
    4c4d4e4f 48494a4b 44454647 40414243
    7c7d7e7f 78797a7b 74757677 70717273
    6c6d6e6f 68696a6b 64656667 60616263
    1c1d1e1f 18191a1b


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    544e257e a2a3e5ea 19a590e6 a24b724c
    e6327757 723fe275 1b75bf00 7d80f6b3
    60744bf1 b7a88ea5 85f9765b 47911976
    d3191cf8 3c039f5f fab0d29c c9d9b6da

--------------------------------------------------------------
Mac is
    544e257e a2a3e5ea 19a590e6 a24b724c
    e6327757 723fe275 1b75bf00 7d80f6b3
    60744bf1 b7a88ea5 85f9765b 47911976
    d3191cf8 3c039f5f fab0d29c c9d9b6da

==============================================================
Sample #3

Block length = 72

Key length = 136

Tag length = 64

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
--------------------------------------------------------------
K0 is
    ad8edff4 f1b7aa1c 63bbe497 28ab9b16
    5f7245b3 d7102e6f 99c261fc 15d2d0bf
    6afef6a4 91720454 a1349fbf 5d848854
    875ac83a 1156fd7f 6e2a37af 26c07fb2
    00000000 00000000

K0 xor ipad is
    9bb8e9c2 c7819c2a 558dd2a1 1e9dad20
    69447385 e1261859 aff457ca 23e4e689
    5cc8c092 a7443262 9702a989 6bb2be62
    b16cfe0c 2760cb49 581c0199 10f64984
    36363636 36363636

Hash((Key^ipad)||text) is
    6d6c25a2 05eecb57 f2bd9524 c56516b2
    57ce7c7c 36342016 baf69e99 78cdea31
    13c62277 48437a00 dba063f9 e8c7955f
    7124620e cc8bbec1 ce6a40d0 328c13f6
```

```
K0 xor opad is
   f1d283a8 adebf640 3fe7b8cb 74f7c74a
   032e19ef 8b4c7233 c59e3da0 498e8ce3
   36a2aaf8 cd2e5808 fd68c3e3 01d8d408
   db069466 4d0aa123 32766bf3 7a9c23ee
   5c5c5c5c 5c5c5c5c


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
   5f464f5e 5b7848e3 885e49b2 c385f069
   4985d0e3 8966242d c4a5fe3f ea4b37d4
   6b65cece d5dcf594 38dd840b ab22269f
   0ba7febd b9fcf746 02a35666 b2a32915

--------------------------------------------------------------
Mac is
   5f464f5e 5b7848e3 885e49b2 c385f069
   4985d0e3 8966242d c4a5fe3f ea4b37d4
   6b65cece d5dcf594 38dd840b ab22269f
   0ba7febd b9fcf746 02a35666 b2a32915

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

Sample #4

Block length = 72

Key length = 64

Tag length = 32

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
   30313233 34353637 38393a3b 3c3d3e3f
```

```
--------------------------------------------------------------
K0 is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 1c1d1e1f
    20212223 24252627 28292a2b 2c2d2e2f
    30313233 34353637 38393a3b 3c3d3e3f
    00000000 00000000

K0 xor ipad is
    36373435 32333031 3e3f3c3d 3a3b3839
    26272425 22232021 2e2f2c2d 2a2b2829
    16171415 12131011 1e1f1c1d 1a1b1819
    06070405 02030001 0e0f0c0d 0a0b0809
    36363636 36363636

Hash((Key^ipad)||text) is
    954f6b21 55a6c560 fd2c3145 2047c3a6
    d74ed2be cc700e60 047efffb f2752ed0
    2e998db3 9639312d a8a89e17 5de9d8c6
    4a92b48f 415e415c 3a4a02d2 fe2d09ec

K0 xor opad is
    5c5d5e5f 58595a5b 54555657 50515253
    4c4d4e4f 48494a4b 44454647 40414243
    7c7d7e7f 78797a7b 74757677 70717273
    6c6d6e6f 68696a6b 64656667 60616263
    5c5c5c5c 5c5c5c5c


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    7bb06d85 9257b25c e73ca700 df34c5cb
    ef5c898b ac91029e 0b27975d 4e526a08
    8f5e590e e736969f 445643a5 8bee7ee0
    cbbbb2e1 47755844 35d36ad0 de6b9499

--------------------------------------------------------------
Mac is
    7bb06d85 9257b25c e73ca700 df34c5cb
    ef5c898b ac91029e 0b27975d 4e526a08
```