```
##############################################################

    Keyed-Hash Message Authentication Code (HMAC)
       using SHA3-224

      Hashlen = 28

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

Sample #1

Block length = 144

Key length = 28

Tag length = 28

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

K0 xor ipad is
    36373435 32333031 3e3f3c3d 3a3b3839
    26272425 22232021 2e2f2c2d 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 36363636 36363636 36363636

Hash((Key^ipad)||text) is
    74e88803 4e39b3ec f12abdcd cb0de0e7
    696b09cc 6251c9ad c5752d4d

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


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    332cfd59 347fdb8e 576e7726 0be4aba2
    d6dc5311 7b3bfb52 c6d18c04
--------------------------------------------------------------
Mac is
    332cfd59 347fdb8e 576e7726 0be4aba2
    d6dc5311 7b3bfb52 c6d18c04
==============================================================

Sample #2

Block length = 144

Key length = 144

Tag length = 28

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 88898a8b 8c8d8e8f

--------------------------------------------------------------
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 88898a8b 8c8d8e8f

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 bebfbcbd babbb8b9

Hash((Key^ipad)||text) is
    872c8246 819f0760 6bcb4422 81879a5a
    7ff6d973 51cff0ed 97bd4aef

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 d4d5d6d7 d0d1d2d3
```

```
Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    d8b733bc f66c644a 12323d56 4e24dcf3
    fc75f231 f3b67968 359100c7
--------------------------------------------------------------
Mac is
    d8b733bc f66c644a 12323d56 4e24dcf3
    fc75f231 f3b67968 359100c7
==============================================================

Sample #3

Block length = 144

Key length = 172

Tag length = 28

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 a8a9aaab
--------------------------------------------------------------
K0 is
    46f9d06d 9d45a89c f79ada60 2f77f392
    36114945 e41abba6 56a122cb 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 00000000 00000000 00000000

K0 xor ipad is
    70cfe65b ab739eaa c1acec56 1941c5a4
    00277f73 d22c8d90 609714fd 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 36363636 36363636 36363636

Hash((Key^ipad)||text) is
    a35378e9 b9c5d3df 92a21925 d35ba01b
    5dd15d0a d3b08489 86576125

K0 xor opad is
    1aa58c31 c119f4c0 abc6863c 732bafce
    6a4d1519 b846e7fa 0afd7e97 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 5c5c5c5c 5c5c5c5c 5c5c5c5c


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    078695ee cc227c63 6ad31d06 3a15dd05
    a7e819a6 6ec6d8de 1e193e59
--------------------------------------------------------------
Mac is
    078695ee cc227c63 6ad31d06 3a15dd05
    a7e819a6 6ec6d8de 1e193e59
==============================================================

Sample #4

Block length = 144

Key length = 28

Tag length = 14
```

```
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
--------------------------------------------------------------
K0 is
    00010203 04050607 08090a0b 0c0d0e0f
    10111213 14151617 18191a1b 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 00000000 00000000 00000000

K0 xor ipad is
    36373435 32333031 3e3f3c3d 3a3b3839
    26272425 22232021 2e2f2c2d 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 36363636 36363636 36363636

Hash((Key^ipad)||text) is
    5c6ad205 86a267ae 0dac60db 9781cc29
    c1337c09 14d9150a df7a895d

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


Hash((K0^opad)||Hash((K0^ipad)||text)) is:
    8569c54c bb00a9b7 8ff1b391 b0e5cd2f
    a5ec7285 50aa3979 703305d4
-------------------------------------------------------
Mac is
    8569c54c bb00a9b7 8ff1b391 b0e5
```