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

  Keyed-Hash Message Authentication Code (HMAC)

    Hashlen = 384

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

Key length = 128

Tag length = 48

Input Date:
        "Sample message for keylen=blocklen"

Text is
                                        5361 6D706C65 206D6573
        73616765 20666F72 206B6579 6C656E3D 626C6F63 6B6C656E


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


----------------------------------------------------------------
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


K0^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
```

```
Hash((Key^ipad)||text) is
        DEE971C9 DCE626E2 27E4DAB9 D01F93DD 7F16D992 F100F518
        D30A288A A3C3B993 3788E0D0 3798FDF5 ACF14B78 C93D402B


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


Hash((K0^opad)||Hash((K0^ipad)||text)) is
        63C5DAA5 E651847C A897C958 14AB830B EDEDC7D2 5E83EEF9
        195CD458 57A37F44 8947858F 5AF50CC2 B1B730DD F29671A9


-------------------------------------------------------------
mac is
        63C5DAA5 E651847C A897C958 14AB830B EDEDC7D2 5E83EEF9
        195CD458 57A37F44 8947858F 5AF50CC2 B1B730DD F29671A9


=============================================================
Key length = 48

Tag length = 48

Input Date:
        "Sample message for keylen<blocklen"

Text is
                                      5361 6D706C65 206D6573
        73616765 20666F72 206B6579 6C656E3C 626C6F63 6B6C656E


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
        00000000 00000000 00000000 00000000 00000000 00000000


K0^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
        36363636 36363636 36363636 36363636 36363636 36363636


Hash((Key^ipad)||text) is
        AC721E61 3E4FE953 8B60D943 DF27C979 B0DC18BE 9E835580
        38BFF203 6594F228 53B363E0 F50A1B55 88957327 9ACDDAF8


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
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
        6EB242BD BB582CA1 7BEBFA48 1B1E2321 1464D2B7 F8C20B9F
        F2201637 B93646AF 5AE9AC31 6E98DB45 D9CAE773 675EEED0


-----------------------------------------------------------------
mac is
        6EB242BD BB582CA1 7BEBFA48 1B1E2321 1464D2B7 F8C20B9F
        F2201637 B93646AF 5AE9AC31 6E98DB45 D9CAE773 675EEED0


=================================================================
Key length = 200
```

```
Tag length = 48

Input Date:
        "Sample message for keylen=blocklen"

Text is
                                        5361 6D706C65 206D6573
        73616765 20666F72 206B6579 6C656E3D 626C6F63 6B6C656E


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 ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


---------------------------------------------------------------
K0 is
                                             7EA4BB25 34C67036
        F49DE7BE B5FE8A24 78DF04FF 3FEF40A9 CD492399 9A590E99
        12DF1297 217CE1A0 21AA2FB1 013498B8 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


K0^ipad is
                                             48928D13 02F04600
        C2ABD188 83C8BC12 4EE932C9 09D9769F FB7F15AF AC6F38AF
        24E924A1 174AD796 179C1987 3702AE8E 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
        01418D09 30D04496 E8B409D5 F4E0C45A 63CFED0F C56C952E
        9B3C7599 03B25567 60DEE915 A55E40B5 9BD9BA09 91A3163C
```

```
K0 xor opad is
                                                22F8E779 689A2C6A
        A8C1BBE2 E9A2D678 248358A3 63B31CF5 91157FC5 C60552C5
        4E834ECB 7D20BDFC 7DF673ED 5D68C4E4 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
        5B664436 DF69B0CA 22551231 A3F0A3D5 B4F97991 713CFA84
        BFF4D079 2EFF96C2 7DCCBBB6 F79B65D5 48B40E85 64CEF594


---------------------------------------------------------------
mac is
        5B664436 DF69B0CA 22551231 A3F0A3D5 B4F97991 713CFA84
        BFF4D079 2EFF96C2 7DCCBBB6 F79B65D5 48B40E85 64CEF594


===============================================================
Key length = 49

Tag length = 24

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

Text is
                                                    5361 6D706C65
        206D6573 73616765 20666F72 206B6579 6C656E3C 626C6F63
        6B6C656E 2C207769 74682074 72756E63 61746564 20746167


Key is
                                                              00
        01020304 05060708 090A0B0C 0D0E0F10 11121314 15161718
        191A1B1C 1D1E1F20 21222324 25262728 292A2B2C 2D2E2F30


---------------------------------------------------------------
K0 is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 28292A2B 2C2D2E2F 30000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

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


K0^ipad is
                                                36373435 32333031
        3E3F3C3D 3A3B3839 26272425 22232021 2E2F2C2D 2A2B2829
        16171415 12131011 1E1F1C1D 1A1B1819 06363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636


Hash((Key^ipad)||text) is
        1D5FFA84 C27ED78A 427FD0CF 94CA0F82 1DDAF1E9 3053A8B3
        D85725D6 0EC2215B 15AAB4AD 14573E75 4A8C1D97 60587F9E


K0 xor opad is
                                                5C5D5E5F 58595A5B
        54555657 50515253 4C4D4E4F 48494A4B 44454647 40414243
        7C7D7E7F 78797A7B 74757677 70717273 6C5C5C5C 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
        C48130D3 DF703DD7 CDAA5680 0DFBD2BA 2458320E 6E1F98FE
        C8AD9F57 F43800DF 3615CEB1 9AB648E1 ECDD8C73 0AF95C8A


---------------------------------------------------------------
mac is
        C48130D3 DF703DD7 CDAA5680 0DFBD2BA 2458320E 6E1F98FE
```