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

  Keyed-Hash Message Authentication Code (HMAC)

    Hashlen = 160

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

Key length = 64

Tag length = 20

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


----------------------------------------------------------------
K0 is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
        28292A2B 2C2D2E2F 30313233 34353637 38393A3B 3C3D3E3F


K0^ipad is
                          36373435 32333031 3E3F3C3D 3A3B3839
        26272425 22232021 2E2F2C2D 2A2B2829 16171415 12131011
        1E1F1C1D 1A1B1819 06070405 02030001 0E0F0C0D 0A0B0809


Hash((Key^ipad)||text) is
                8F51A3BB 9E96B972 59A90921 321F538A DF4A343D


K0 xor opad is
                          5C5D5E5F 58595A5B 54555657 50515253
        4C4D4E4F 48494A4B 44454647 40414243 7C7D7E7F 78797A7B
```

```
        74757677 70717273 6C6D6E6F 68696A6B 64656667 60616263


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                5FD596EE 78D5553C 8FF4E72D 266DFD19 2366DA29


---------------------------------------------------------------
mac is
                5FD596EE 78D5553C 8FF4E72D 266DFD19 2366DA29


===============================================================
Key length = 20

Tag length = 20

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


---------------------------------------------------------------
K0 is
                         00010203 04050607 08090A0B 0C0D0E0F
        10111213 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


K0^ipad is
                         36373435 32333031 3E3F3C3D 3A3B3839
        26272425 36363636 36363636 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636


Hash((Key^ipad)||text) is
                13DE01B7 AD467D75 6FBA1EA8 16866E32 416A269D
```

```
K0 xor opad is
                          5C5D5E5F 58595A5B 54555657 50515253
        4C4D4E4F 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                 4C99FF0C B1B31BD3 3F8431DB AF4D17FC D356A807


---------------------------------------------------------------
mac is
                 4C99FF0C B1B31BD3 3F8431DB AF4D17FC D356A807


===============================================================
Key length = 100

Tag length = 20

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


---------------------------------------------------------------
K0 is
                          1E6634BF AEBC0348 29810592 3D0F26E4
        7AA33FF5 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


K0^ipad is
                          28500289 988A357E 1FB733A4 0B3910D2
        4C9509C3 36363636 36363636 36363636 36363636 36363636
```

```
        36363636 36363636 36363636 36363636 36363636 36363636


Hash((Key^ipad)||text) is
                6487C866 A66F67A2 218B8E89 8892F9E8 282023D2


K0 xor opad is
                         423A68E3 F2E05F14 75DD59CE 61537AB8
        26FF63A9 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                2D51B2F7 750E4105 84662E38 F133435F 4C4FD42A


----------------------------------------------------------------
mac is
                2D51B2F7 750E4105 84662E38 F133435F 4C4FD42A


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

Tag length = 12

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


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


Hash((Key^ipad)||text) is
                65B451E5 30BF4E5D D6EF3891 861D5C82 CEEF5843


K0 xor opad is
                         5C5D5E5F 58595A5B 54555657 50515253
        4C4D4E4F 48494A4B 44454647 40414243 7C7D7E7F 78797A7B
        74757677 70717273 6C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                FE352956 5CD8E28C 5FA79EAC 9D8023B5 3B289D96


---------------------------------------------------------------
mac is
                                  FE352956 5CD8E28C 5FA79EAC
```