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

  Keyed-Hash Message Authentication Code (HMAC)

    Hashlen = 224

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

Key length = 64

Tag length = 28

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
                                                     8D993002
        FF74C1E8 5C28C0C8 B5FB220E 9EE7CEB9 621270BF A1EF0F7C


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
                                                     C7405E3A
        E058E8CD 30B08B41 40248581 ED174CB3 4E1224BC C1EFC81B


----------------------------------------------------------------
mac is
                                                     C7405E3A
        E058E8CD 30B08B41 40248581 ED174CB3 4E1224BC C1EFC81B


================================================================
Key length = 28

Tag length = 28

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


----------------------------------------------------------------
K0 is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


K0^ipad is
                          36373435 32333031 3E3F3C3D 3A3B3839
        26272425 22232021 2E2F2C2D 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636
```

```
Hash((Key^ipad)||text) is
                                                     E6242C93
        AD4D7159 AA0234D4 DD5805C2 D3AC3347 977A8D97 3BFA4081


K0 xor opad is
                          5C5D5E5F 58595A5B 54555657 50515253
        4C4D4E4F 48494A4B 44454647 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                                                     E3D249A8
        CFB67EF8 B7A169E9 A0A59971 4A2CECBA 65999A51 BEB8FBBE


--------------------------------------------------------------
mac is
                                                     E3D249A8
        CFB67EF8 B7A169E9 A0A59971 4A2CECBA 65999A51 BEB8FBBE


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

Tag length = 28

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
                          6E08215B 5470DDEB 67E44A49 4E52E259
        A9C2C4FB ED4AF5DC 6DB3E92A 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


K0^ipad is
                          583E176D 6246EBDD 51D27C7F 7864D46F
        9FF4F2CD DB7CC3EA 5B85DF1C 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636


Hash((Key^ipad)||text) is
                                                     5FBAE182
        DA6789EF F04F242B DC572DD6 67C9DEED F2FE9DC7 8A72EE7F


K0 xor opad is
                          32547D07 082C81B7 3BB81615 120EBE05
        F59E98A7 B116A980 31EFB576 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                                                     91C52509
        E5AF8531 601AE623 0099D90B EF88AAEF B961F408 0ABC014D


--------------------------------------------------------------
mac is
                                                     91C52509
        E5AF8531 601AE623 0099D90B EF88AAEF B961F408 0ABC014D


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

Tag length = 16

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
                                                     F74EBAF6
        1394F4D9 14A54DAD ED03D873 5A8EB7D5 E4F37E43 6861495F


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
                                                     D522F1DF
        596CA4B4 B1C23D27 BDE067D6 153BA972 5FD5CDE0 AF4A2A42


--------------------------------------------------------------
mac is
                          D522F1DF 596CA4B4 B1C23D27 BDE067D6
```