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

  Keyed-Hash Message Authentication Code (HMAC)

    Hashlen = 256

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

Key length = 64

Tag length = 32

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
                                               C0918E14 C43562B9
        10DB4B81 01CF8812 C3DA2783 C670BFF3 4D88B3B8 8E731716


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
                                                 8BB9A1DB 9806F20D
        F7F77B82 138C7914 D174D59E 13DC4D01 69C9057B 133E1D62


-------------------------------------------------------------
mac is
                                                 8BB9A1DB 9806F20D
        F7F77B82 138C7914 D174D59E 13DC4D01 69C9057B 133E1D62


=============================================================
Key length = 32

Tag length = 32

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


-------------------------------------------------------------
K0 is
                         00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


K0^ipad is
                         36373435 32333031 3E3F3C3D 3A3B3839
        26272425 22232021 2E2F2C2D 2A2B2829 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636
```

```
Hash((Key^ipad)||text) is
                                                B3C52720 B330A1D3
        C4D8B594 A9A73D20 7ED02EE5 078A4A42 2258BD65 14070A5F


K0 xor opad is
                          5C5D5E5F 58595A5B 54555657 50515253
        4C4D4E4F 48494A4B 44454647 40414243 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                                                A28CF431 30EE696A
        98F14A37 678B56BC FCBDD9E5 CF69717F ECF5480F 0EBDF790


---------------------------------------------------------------
mac is
                                                A28CF431 30EE696A
        98F14A37 678B56BC FCBDD9E5 CF69717F ECF5480F 0EBDF790


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

Tag length = 32

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
                          BCE0AFF1 9CF5AA6A 7469A30D 61D04E43
```

```
        76E4BBF6 381052EE 9E7F3392 5C954D52 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


K0^ipad is
                         8AD699C7 AAC39C5C 425F953B 57E67875
        40D28DC0 0E2664D8 A84905A4 6AA37B64 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636


Hash((Key^ipad)||text) is
                                            1E0DFB0C BB61E9F0
        60769E9D F5750129 2426F0DB 58194BC8 5BC63DAC 4670C2C1


K0 xor opad is
                         E0BCF3AD C0A9F636 2835FF51 3D8C121F
        2AB8E7AA 644C0EB2 C2236FCE 00C9110E 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                                            BDCCB6C7 2DDEADB5
        00AE7683 86CB38CC 41C63DBB 0878DDB9 C7A38A43 1B78378D


---------------------------------------------------------------
mac is
                                            BDCCB6C7 2DDEADB5
        00AE7683 86CB38CC 41C63DBB 0878DDB9 C7A38A43 1B78378D


===============================================================
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
                                                 CBA02E36 9D29352F
        BAE86194 4B264187 A7D8C1D2 2CDAF9F5 D746556C FE74DDBE


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
                                                 27A8B157 839EFEAC
        98DF070B 331D5936 18DDB985 D403C0C7 86D23B5D 132E57C7


-------------------------------------------------------------
mac is
                         27A8B157 839EFEAC 98DF070B 331D5936
```