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

  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
```

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

  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
```

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

  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
```

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

  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
```

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

  Keyed-Hash Message Authentication Code (HMAC)

    Hashlen = 512

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

Key length = 128

Tag length = 64

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
                          515C86E0 DD382747 A20BDD27 05AF56C1
        AB87AA1D A14F3EFD D99A5935 08EC520D 60C10643 A3841B1E
        CA7EEFF9 559F5D00 78F93479 58FCA632 1E58769D 15CF3A15


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
                          FC25E240 658CA785 B7A811A8 D3F7B4CA
        48CFA26A 8A366BF2 CD1F836B 05FCB024 BD368530 81811D6C
        EA4216EB AD79DA1C FCB95EA4 586B8A0C E356596A 55FB1347


-----------------------------------------------------------------
mac is
                          FC25E240 658CA785 B7A811A8 D3F7B4CA
        48CFA26A 8A366BF2 CD1F836B 05FCB024 BD368530 81811D6C
        EA4216EB AD79DA1C FCB95EA4 586B8A0C E356596A 55FB1347


=================================================================
Key length = 64

Tag length = 64

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 30313233 34353637 38393A3B 3C3D3E3F


-----------------------------------------------------------
K0 is
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 28292A2B 2C2D2E2F 30313233 34353637
        38393A3B 3C3D3E3F 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 06070405 02030001
        0E0F0C0D 0A0B0809 36363636 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636


Hash((Key^ipad)||text) is
                        DDCB7529 40EDC533 D61AD7A9 0F907AED
        49827F68 FD6514DA 45688AAA 083E03E3 C961D63E 7BAC1B23
        1EA3F78D 63C5A97B 96156202 6C895EF0 51C0F750 679591A9


K0 xor opad is
                                            5C5D5E5F 58595A5B
        54555657 50515253 4C4D4E4F 48494A4B 44454647 40414243
        7C7D7E7F 78797A7B 74757677 70717273 6C6D6E6F 68696A6B
        64656667 60616263 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                        FD44C18B DA0BB0A6 CE0E82B0 31BF2818
        F6539BD5 6EC00BDC 10A8A2D7 30B3634D E2545D63 9B0F2CF7
        10D0692C 72A1896F 1F211C2B 922D1A96 C392E07E 7EA9FEDC


-----------------------------------------------------------
mac is
                        FD44C18B DA0BB0A6 CE0E82B0 31BF2818
```

F6539BD5 6EC00BDC 10A8A2D7 30B3634D E2545D63 9B0F2CF7
10D0692C 72A1896F 1F211C2B 922D1A96 C392E07E 7EA9FEDC

==========

Key length = 200

Tag length = 64

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
986058E9 895E2C2A
B8F9E8CB DF801DB1 2A44842A 56A91D5A 4E87B1FC 98B29372
2C466414 2E42C3C5 51FF8986 46268CD9 2B84ED23 0B8C94BE
D7798D4F 27CD7465 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

K0^ipad is
AE566EDF BF681A1C
8ECFDEFD E9B62B87 1C72B21C 609F2B6C 78B187CA AE84A544
1A705222 1874F5F3 67C9BFB0 7010BAEF 1DB2DB15 3DBAA288
E14FBB79 11FB4253 36363636 36363636 36363636 36363636
36363636 36363636 36363636 36363636 36363636 36363636
36363636 36363636 36363636 36363636 36363636 36363636

```
Hash((Key^ipad)||text) is
                          6DF26817 41D1FE25 F78ED617 188F35C4
        142351B8 A07090AE 7FC7E123 1E5F67A0 D1F14F15 436DD01D
        EECC3E4E 59F9B10A 15DBE69A 6EBF5921 A9428A37 0BA2618D


K0 xor opad is
                                                 C43C04B5 D5027076
        E4A5B497 83DC41ED 7618D876 0AF54106 12DBEDA0 C4EECF2E
        701A3848 721E9F99 0DA3D5DA 1A7AD085 77D8B17F 57D0C8E2
        8B25D113 7B912839 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                          D93EC8D2 DE1AD2A9 957CB9B8 3F14E76A
        D6B5E0CC E285079A 127D3B14 BCCB7AA7 286D4AC0 D4CE6421
        5F2BC9E6 870B33D9 7438BE4A AA20CDA5 C5A912B4 8B8E27F3


---------------------------------------------------------------
mac is
                          D93EC8D2 DE1AD2A9 957CB9B8 3F14E76A
        D6B5E0CC E285079A 127D3B14 BCCB7AA7 286D4AC0 D4CE6421
        5F2BC9E6 870B33D9 7438BE4A AA20CDA5 C5A912B4 8B8E27F3


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

Tag length = 32

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
                          0F70BAB7 04356437 72518C8A 803CB42D
        D3CAEB69 F96C6712 FFB4461A 90FF4900 B3BE2863 AABCCD84
        61D7FD95 3452691B 5F7ACAF1 51A6BC38 5DBFDD3D 97B49C20


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
                          00F3E9A7 7BB0F06D E15F1606 03E42B50
        28758808 596664C0 3E1AB8FB 2B076778 0563AEDC 644960D4
        F0C0C5D2 39F67A2A 61B141E8 C871F3D4 0DB2C605 588DAB92


-------------------------------------------------------------
mac is
```

00F3E9A7 7BB0F06D
E15F1606 03E42B50 28758808 596664C0 3E1AB8FB 2B076778